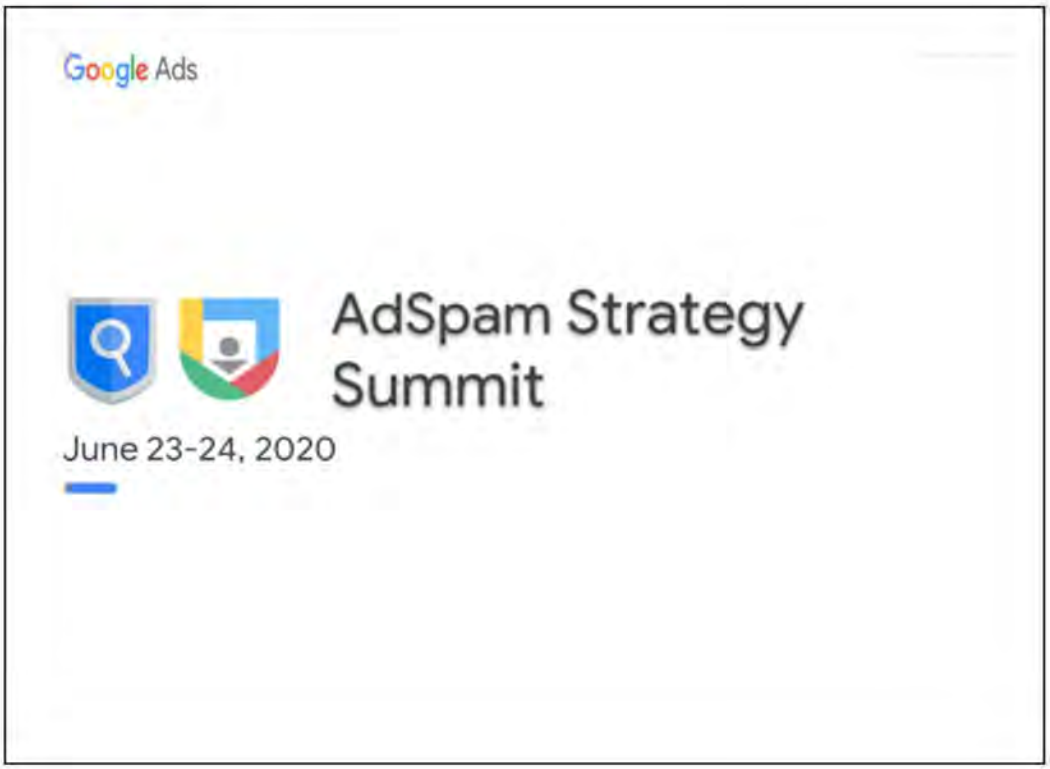
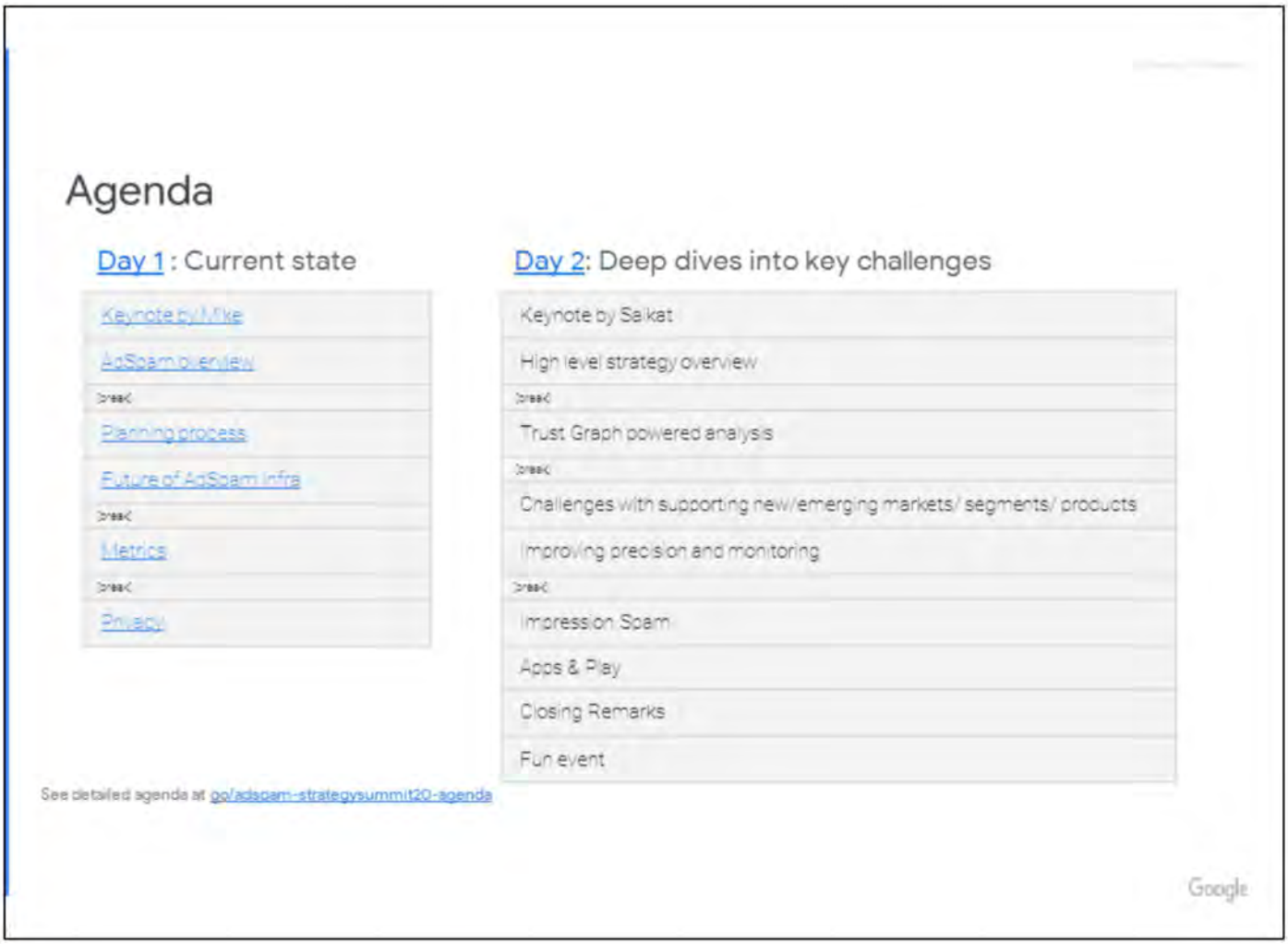
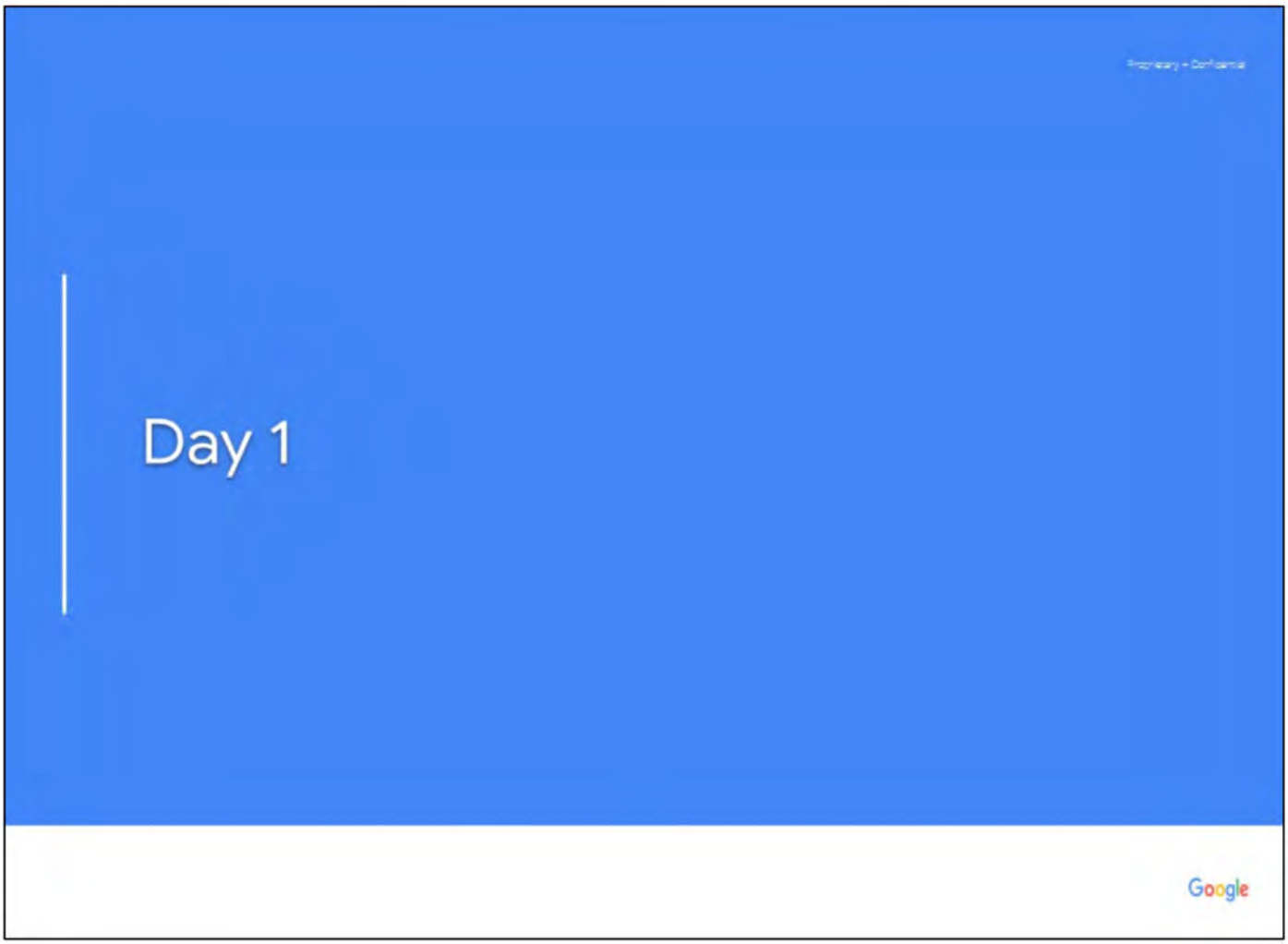


Host: subir

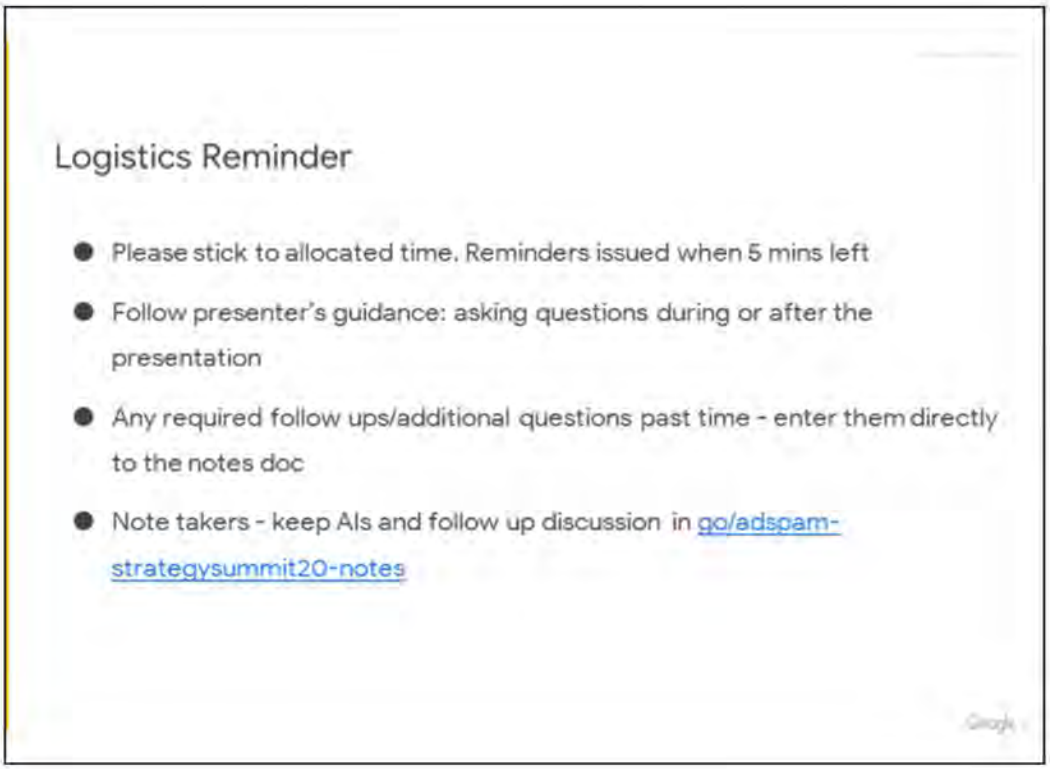

ALL INFORMATION PRESENTED TODAY IS
CONFIDENTIAL
DO NOT SHARE, COPY OR DISTRIBUTE ANY OF THIS CONTENT

Amit

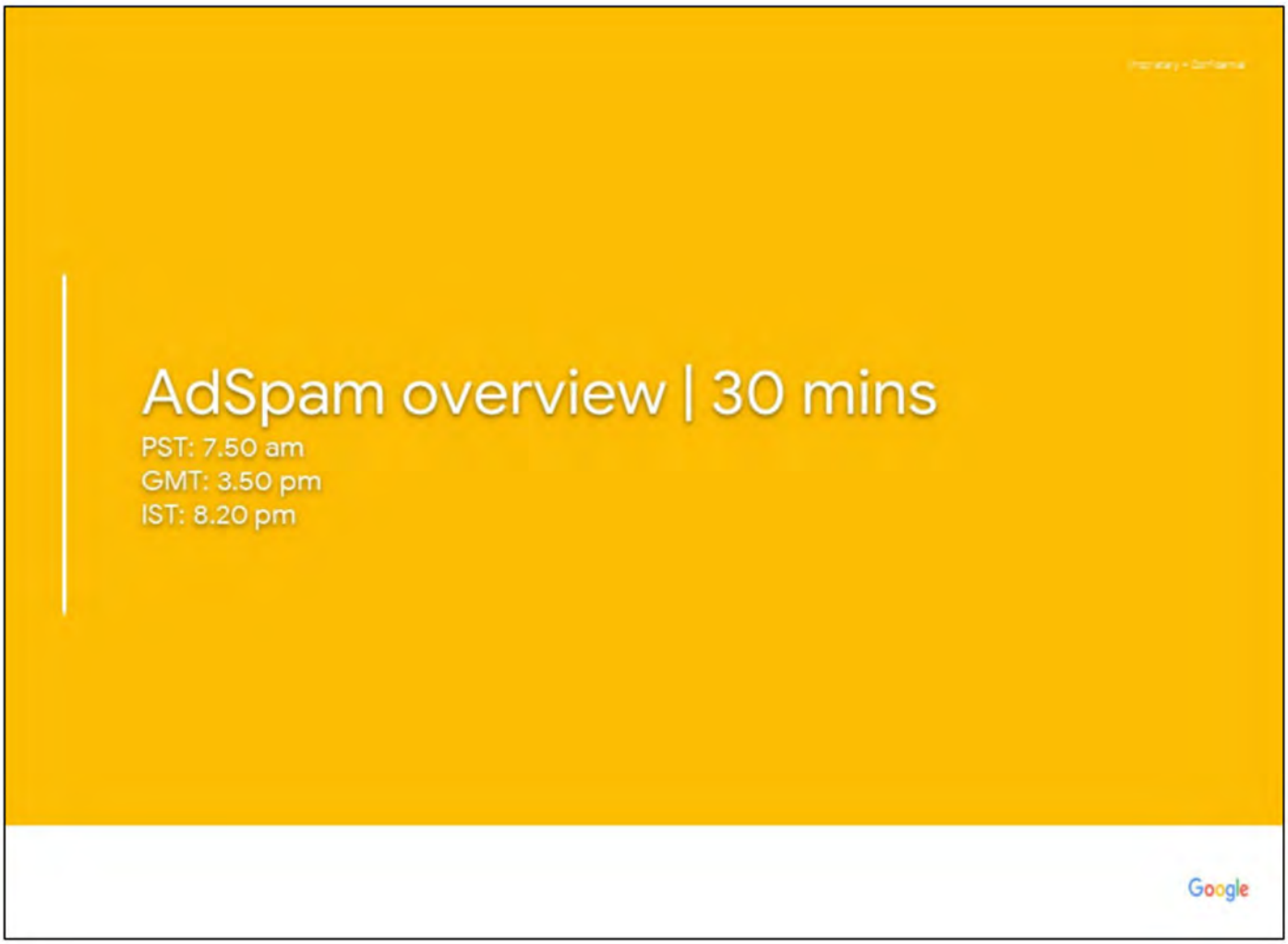

Agenda
Day 1: Current state
Keynote by Mike
AdSpam overview
break
Planning process
Future of AdSpam infra
break
Metrics
break
Privacy
Day 2: Deep dives into key challenges
Keynote by Saikat
High level strategy overview
break
Trust Graph powered analysis
break
Challenges with supporting new/emerging markets/ segments/ products
Improving precision and monitoring
break
Impression Spam
Apps & Play
Closing Remarks
Fun event
See detailed agenda at go/adspam-strategysummit20-agenda
Google

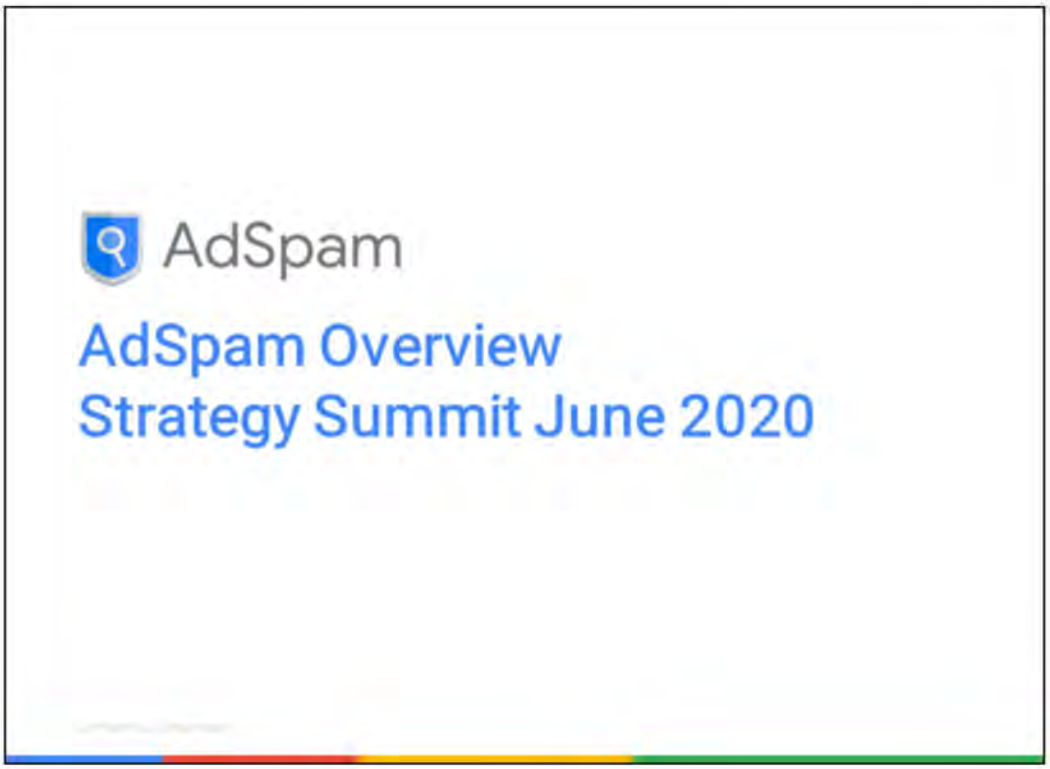

Day 1
Google


Keynote by Mike
PST: 7.30 am
GMT: 3.30 pm
IST: 8.00 pm
Google

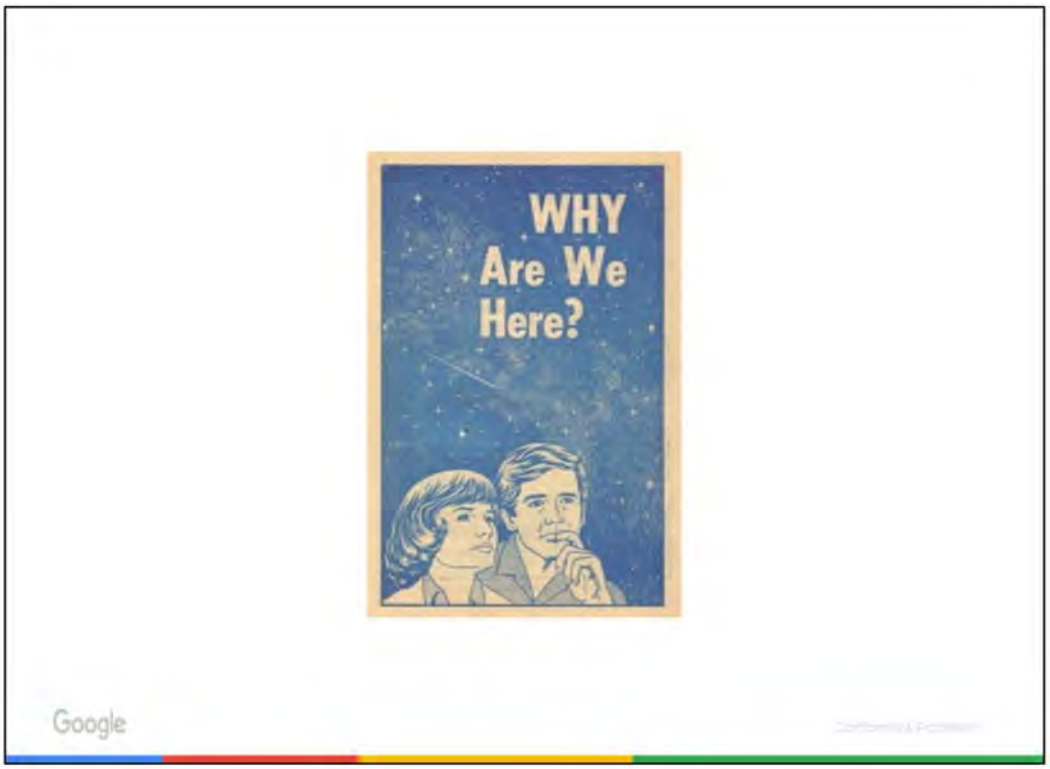

Logistics Reminder
Please stick to allocated time. Reminders issued when 5 mins left
Follow presenter's guidance: asking questions during or after the presentation
Any required follow ups/additional questions past time - enter them directly to the notes doc
Note takers - keep AIs and follow up discussion in go/adspam-strategysummit20-notes

Misha - 40 sec

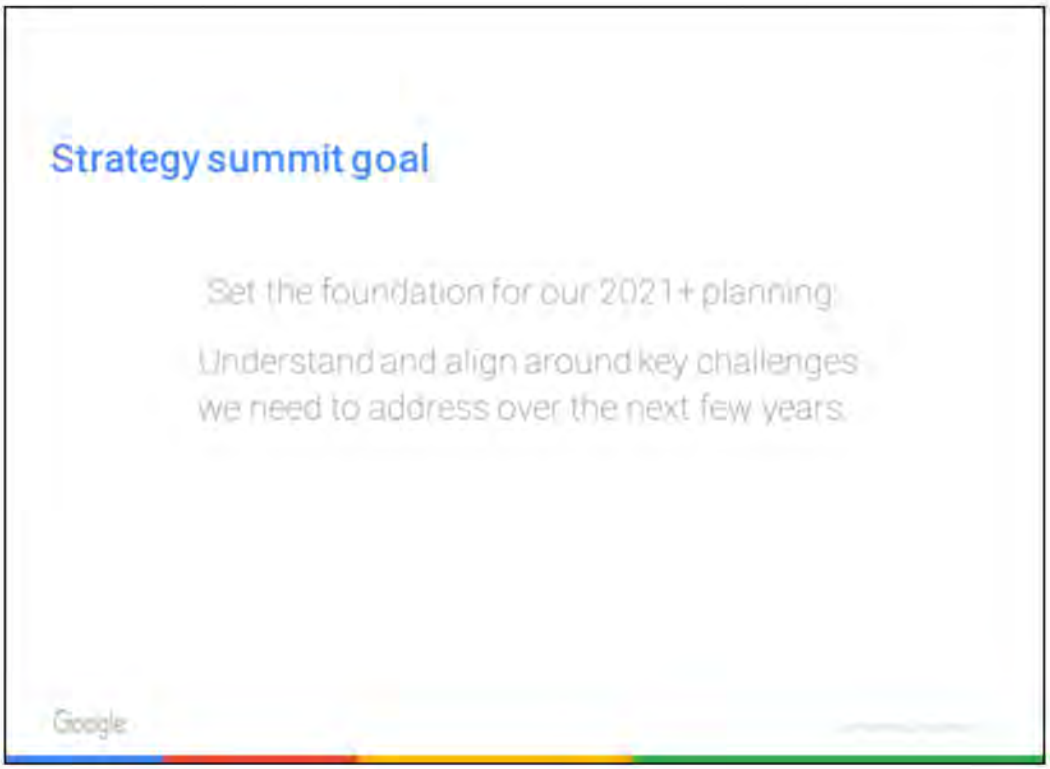

AdSpam overview | 30 mins
PST: 7.50 am
GMT: 3.50 pm
IST: 8.20 pm
Google



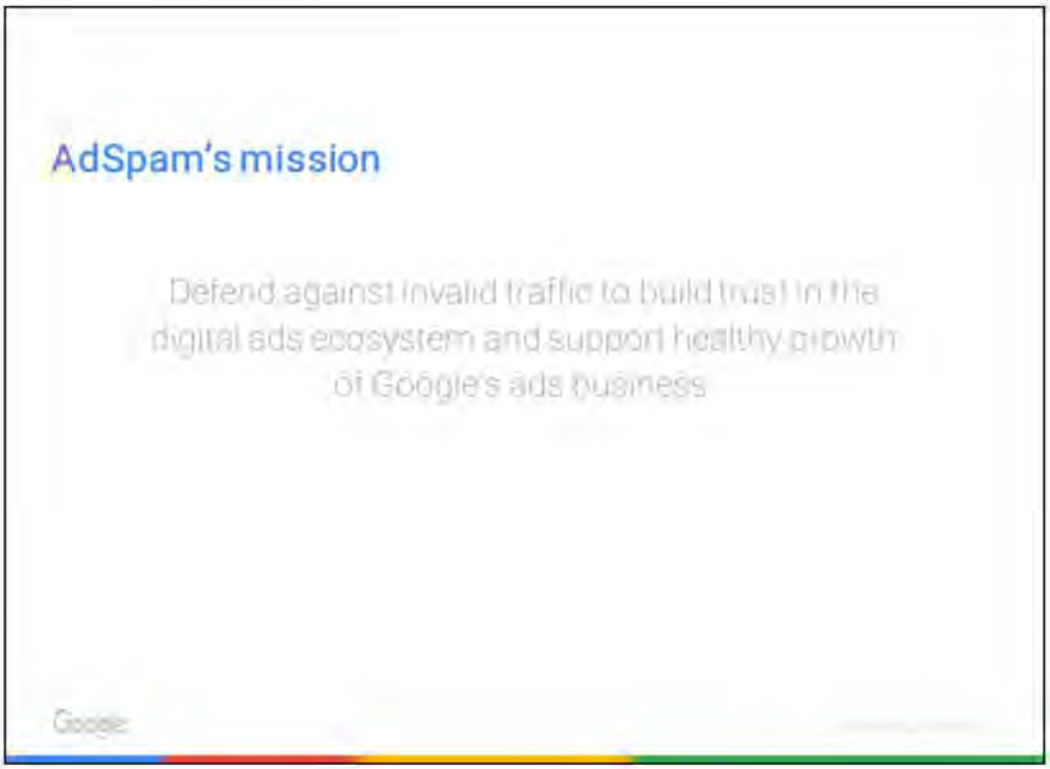
Speaker: Subir



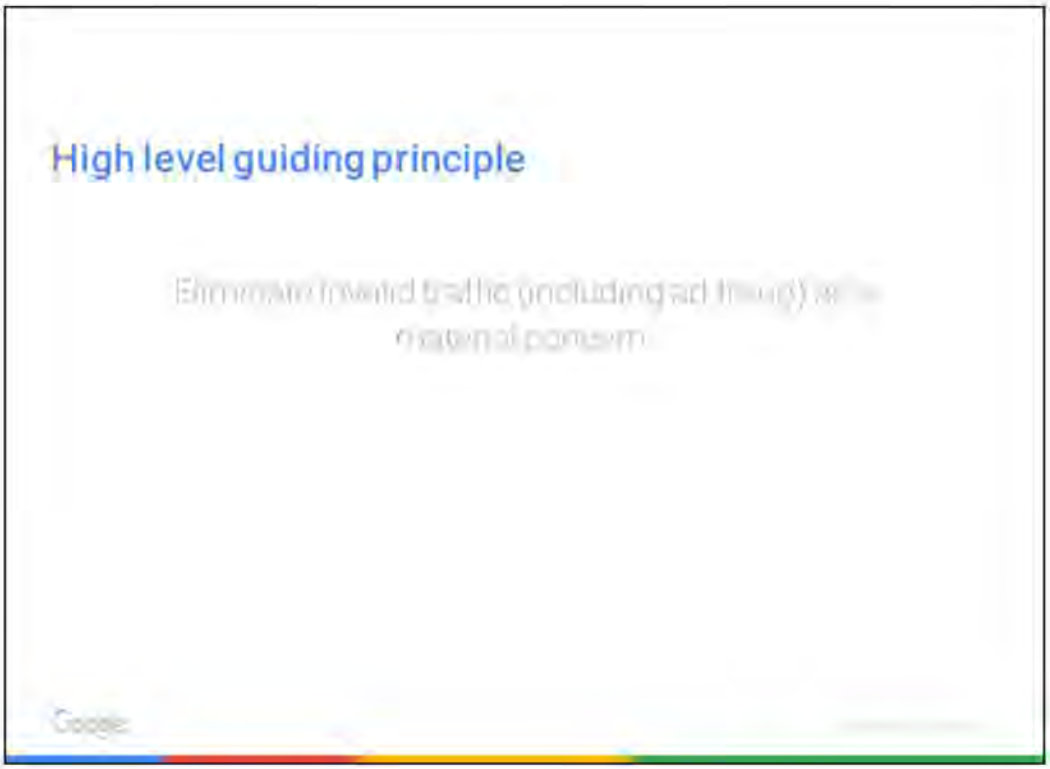
Mission can help answer the big questions...



Alignment on and understanding of key challenges to prepare for 2021 planning (prepare for writing strategy docs for the APaS summit.



The words may be different between how T&S states the mission and how eng states it, but they are both are closely aligned on defending our ads ecosystem against IVT. Puneet explain that T&S' mission closely aligned.



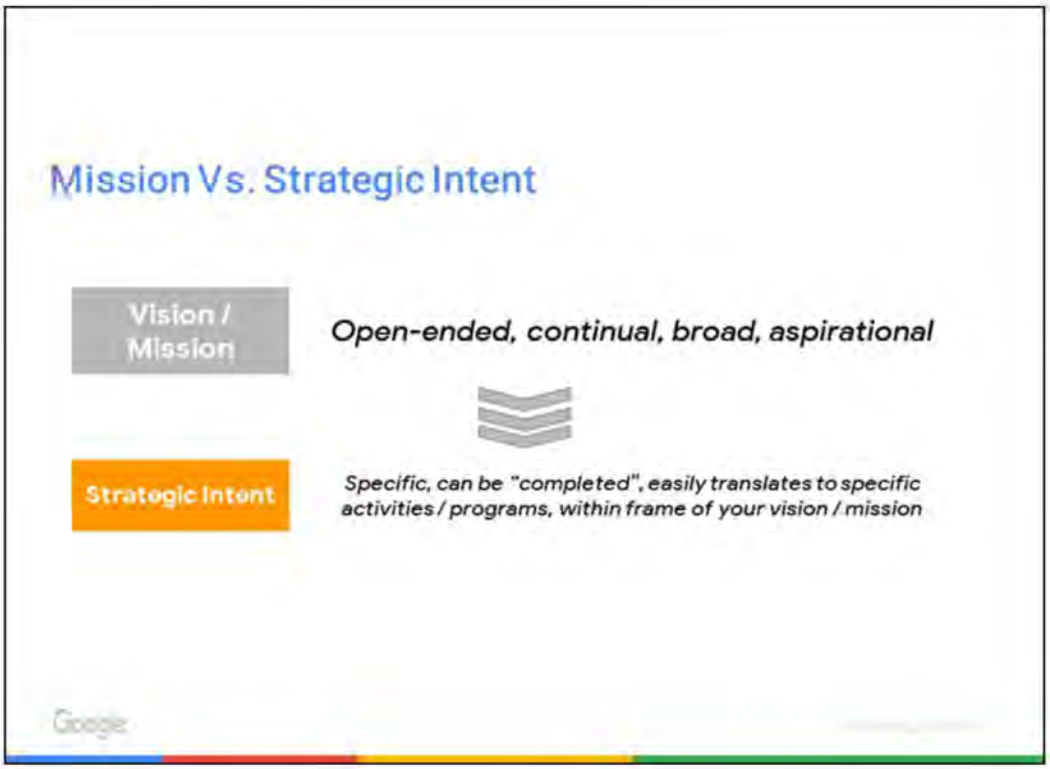
Speaker: Per
Invalid traffic should not be material enough to impact or affect where or how an advertiser allocates budget.

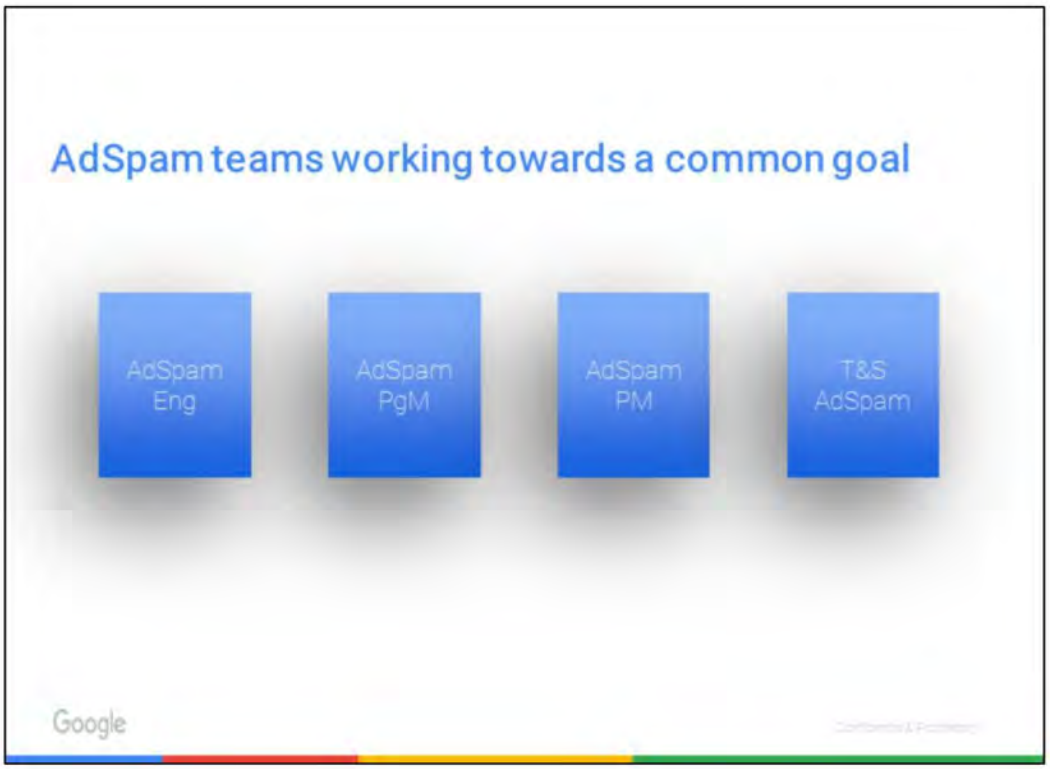
Online advertising ought to get to the same point as some other "mature" areas - for example credit card: As long as you take basic precautions, few credit card holders have material concerns about credit card fraud. Our dream is a future world where advertisers that take basic precautions (e.g., not buy "too cheap to be true" inventory from questionable sources that are not accredited) will not have to worry about invalid traffic and ad fraud in any material way.

Note: As with most other security/fraud areas, we'll "never be completely done". After achieving the "end state" we expect to continue to invest in invalid traffic defenses to maintain that "end state".
Overall guiding principles are available in docs (provide references[1][2])

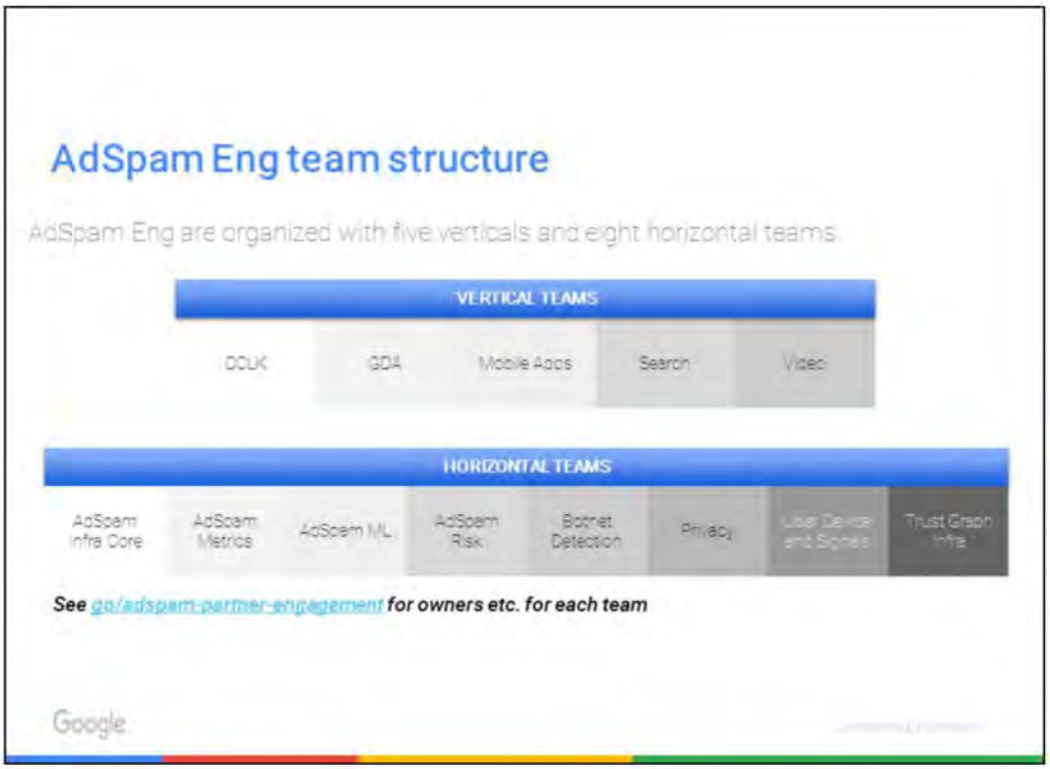
Speaker: Per
This is a bit of a moonshot. Reminder that SI needs to be specific - know when you reach it. Note that this includes defended (aka caught), undefended (aka uncaught), and unknown (see go/adspam-framework for definitions) non-policy invalid traffic; however, since we cannot measure/quantify the unknown category we'll only use defended and undefended as the goal.

Speaker: Per
Mention that we'll do the "work breakdown structure" like for SI - define the next level down and each sub-team will also define their respective SIs.

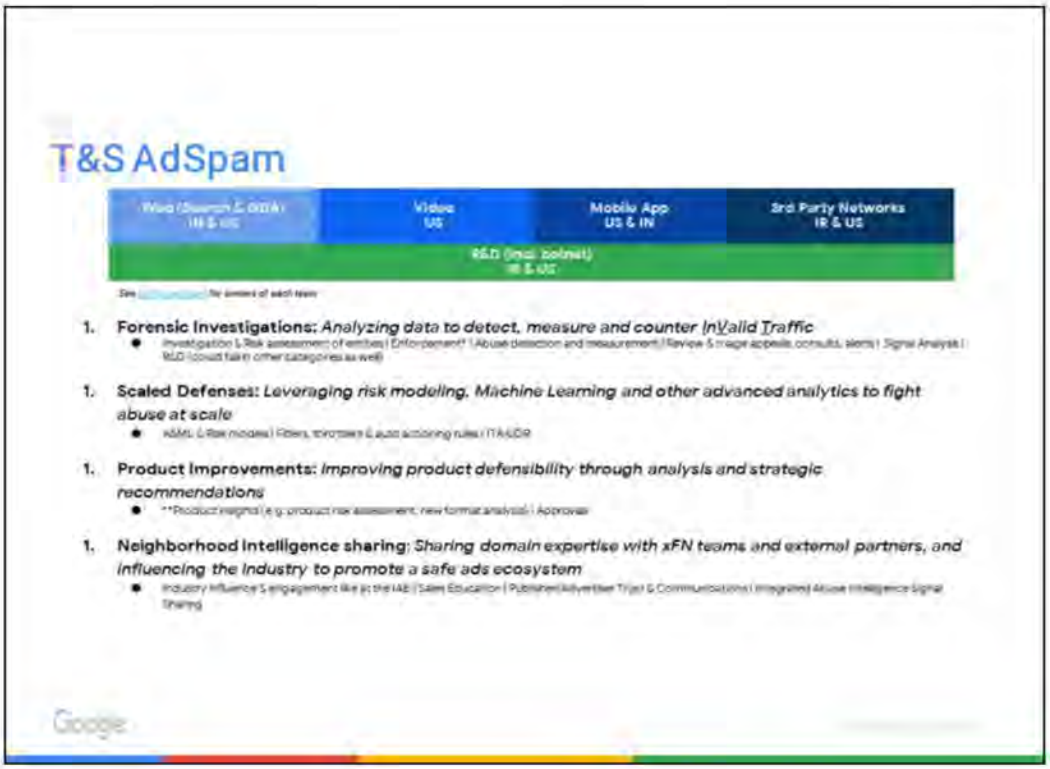

Mission Vs. Strategic Intent
Vision / Mission
Open-ended, continual, broad, aspirational
Strategic Intent
Specific, can be "completed", easily translates to specific activities / programs, within frame of your vision / mission
Google



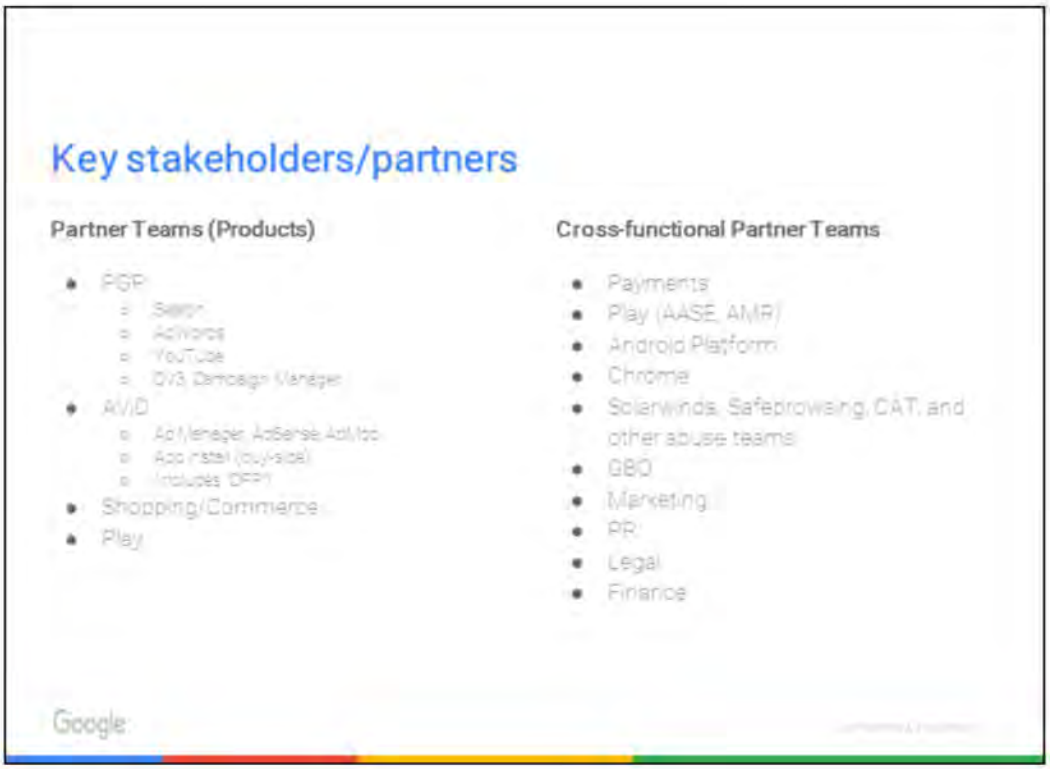
Speaker: Subir



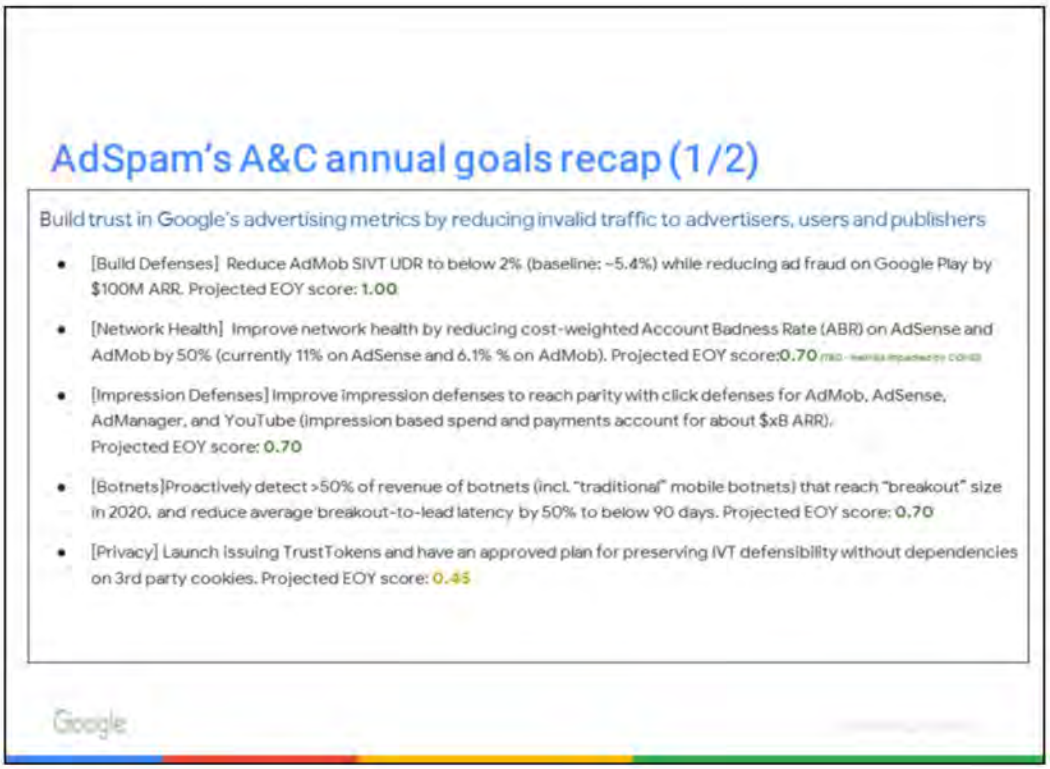
Speaker: Subir



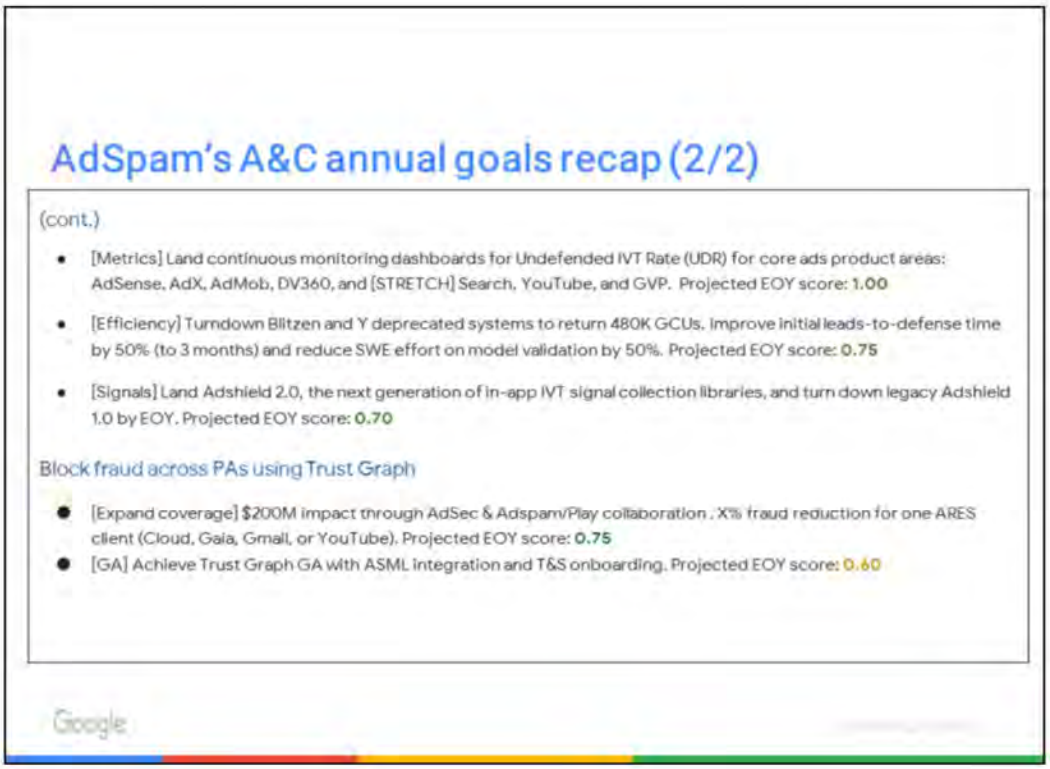
Speaker:Puneet
T&S also organizes itself in verticals & horizontals - 4V & 1H. As you can see, there's many similarities how Eng organizes it. Also have project based WGs like Impression spam and a few others.
What T&S does - categories of work...departure from how we used to call Ops and now this new language.
*Enforcement can include: credits | claw back | termination | zombie | suspension | throttle | warning | reinstate | payment hold | sweeps | blacklist maintenance | contract renewals | workflows / comms | Inbound leads: Appeals | Consults | ML | Governator | Throttling | research | SafetyNet | Escalations | alerts | Smart Leads).
** Product insights can include: product risk assessment, product roadmap, product strategy, new format analysis, tools, cases, contract review, pub comm
Add'l details on each category available here.


Key stakeholders/partners
Partner Teams (Products)
PGP
Search
AdWords
YouTube
DV3 Campaign Manager
AVID
Ad Manager, AdSense, Ad Exchange
App Install (buy-side)
Includes DFP
Shopping/Commerce
Play
Cross-functional Partner Teams
Payments
Play (AASE, AMR)
Android Platform
Chrome
Solarwinds, Safebrowsing, CAT, and other abuse teams
GBO
Marketing
PR
Legal
Finance
Google

Speaker: Per



https://docs.google.com/document/d/1vbI8Vb26gVgeubYqJNWqt41kuTcpODVxWglAfc0ansE/edit#



AdSpam's A&C annual goals recap (2/2)

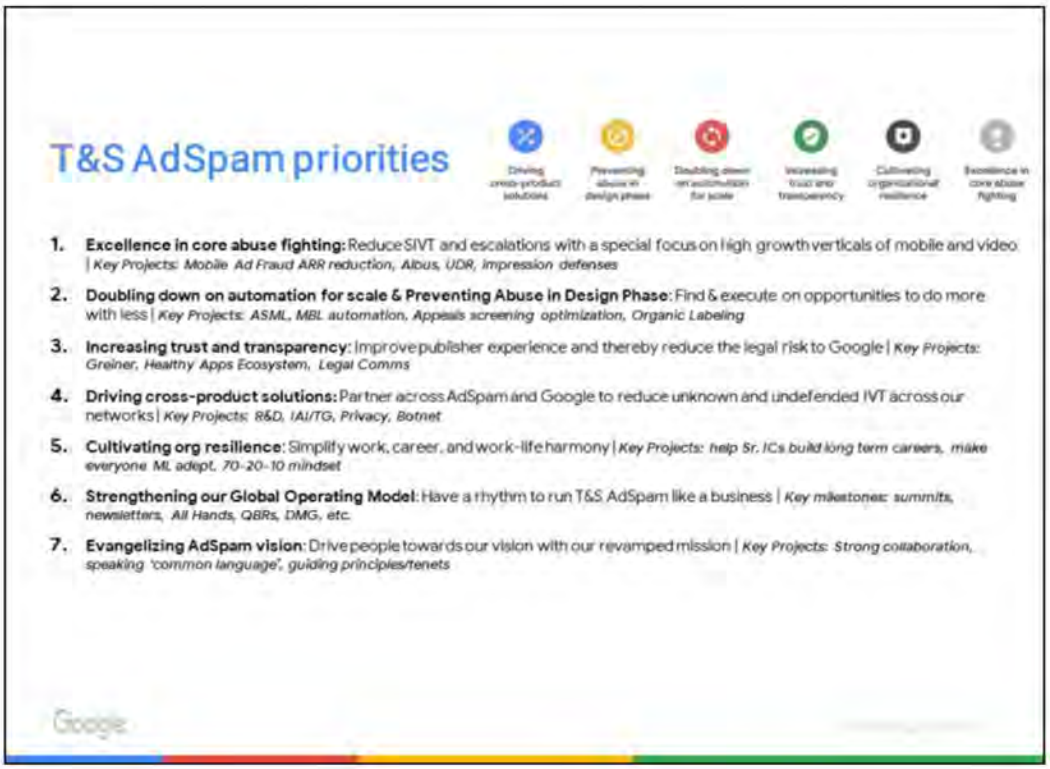
(cont.)

- [Metrics] Land continuous monitoring dashboards for Undefended IVT Rate (UDR) for core ads product areas: AdSense, AdX, AdMob, DV360, and [STRETCH] Search, YouTube, and GVP. Projected EOY score: **1.00**
- [Efficiency] Turndown Blitzen and Y deprecated systems to return 480K GCUs. Improve initial leads-to-defense time by 50% (to 3 months) and reduce SWE effort on model validation by 50%. Projected EOY score: **0.75**
- [Signals] Land Adshield 2.0, the next generation of in-app IVT signal collection libraries, and turn down legacy Adshield 1.0 by EOY. Projected EOY score: **0.70**

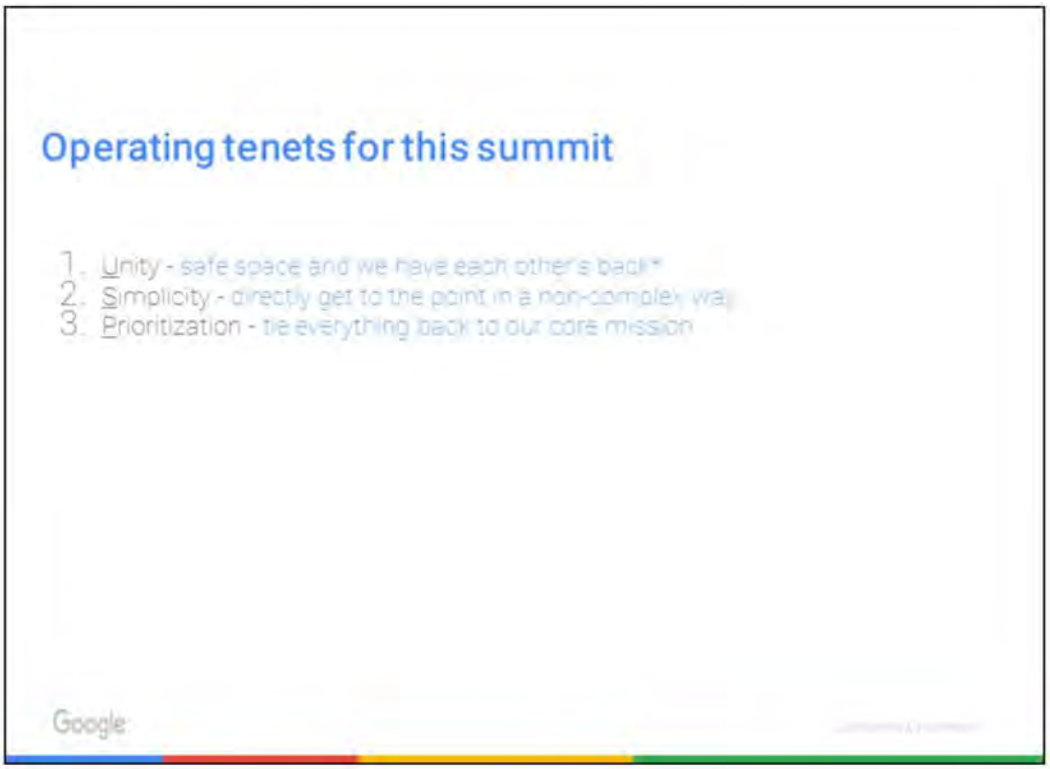
Block fraud across PAs using Trust Graph

- [Expand coverage] $200M impact through AdSec & Adspam/Play collaboration . X% fraud reduction for one ARES client (Cloud, Gaia, Gmail, or YouTube). Projected EOY score: **0.75**
- [GA] Achieve Trust Graph GA with ASML integration and T&S onboarding. Projected EOY score: **0.60**

Google



Speaker Puneet - strategy doc link here
In T&S, we have 7 priorities and aligned with T&S wide 6 pillars.



Speaker: Puneet
*avoid sensitive ppl issues

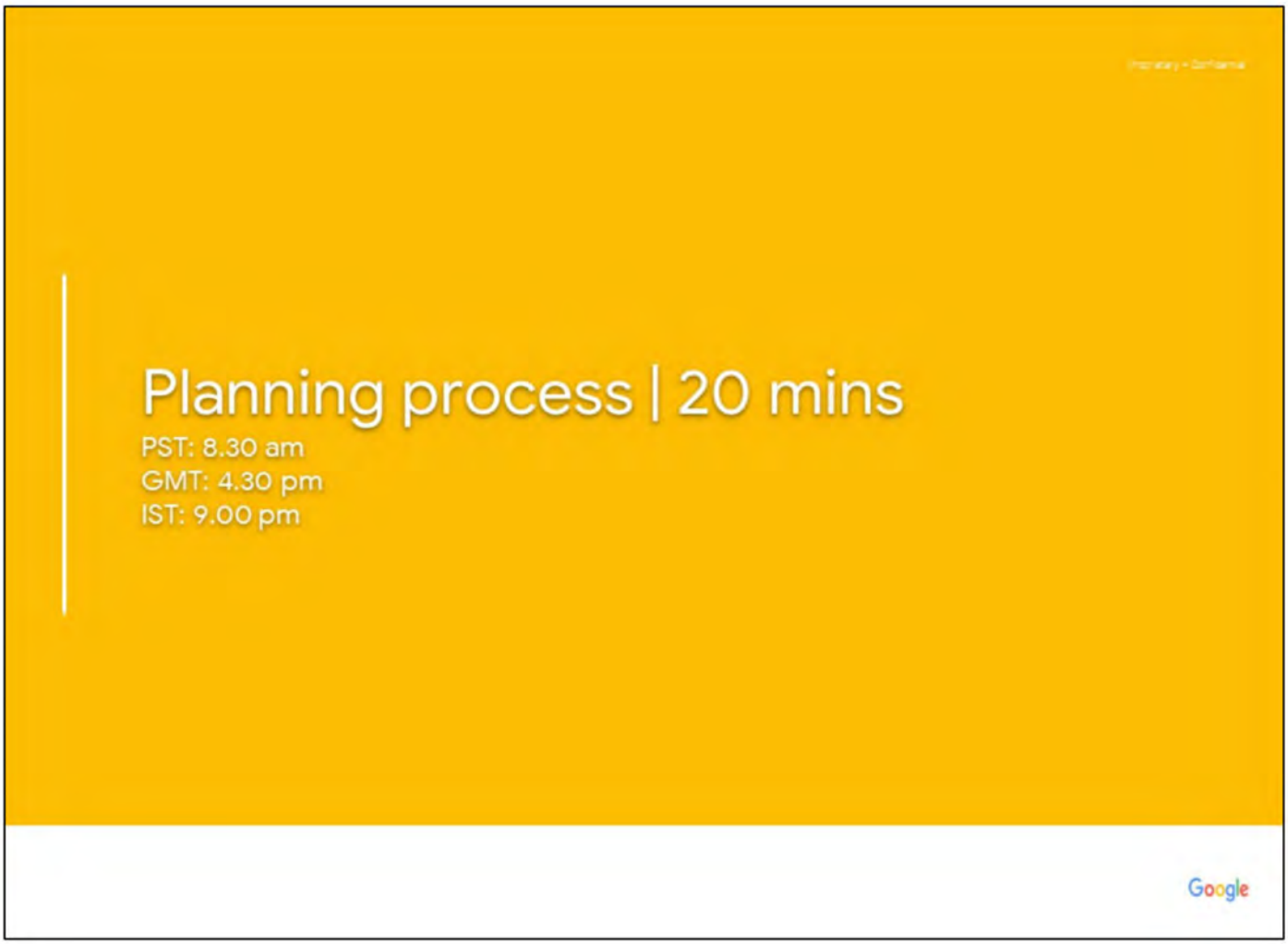
Speaker Puneet
Bonus slide if needed - link to OKRs here quickly skim through the slide as most of it should align with common goals.

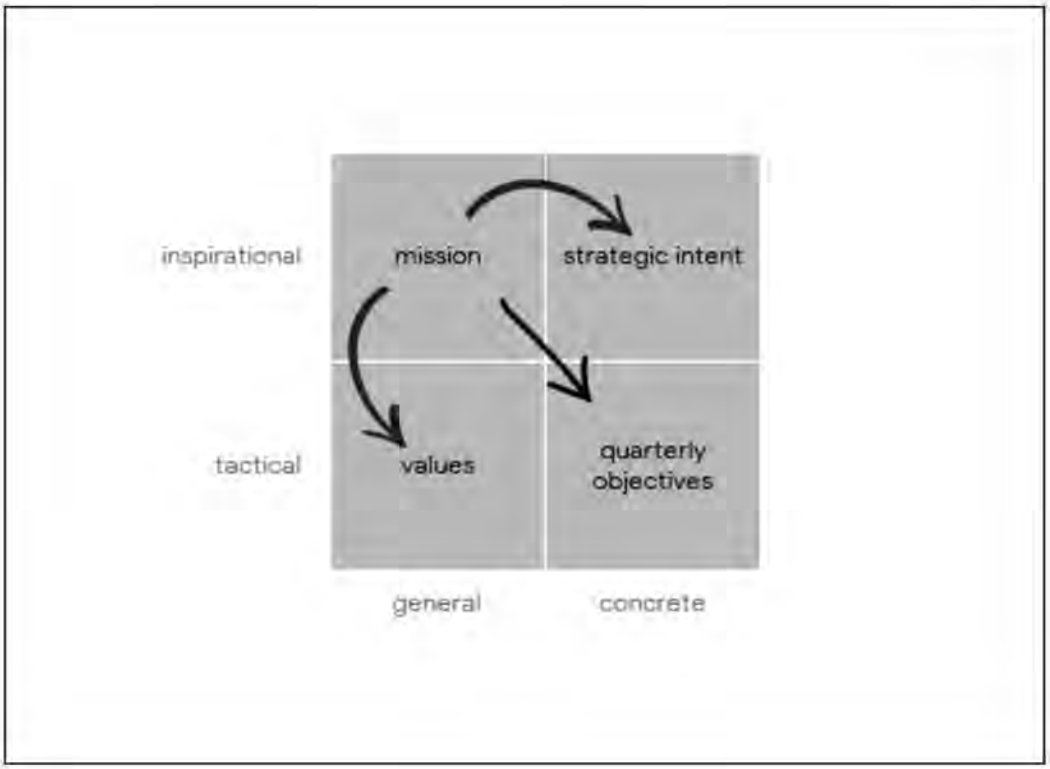
Break | 10 mins

PST: 8.20 - 8.30 am
GMT: 4.20 - 4.30 pm
IST: 8.50-9.00 pm

Next session: Planning process

Google


Planning process | 20 mins
PST: 8.30 am
GMT: 4.30 pm
IST: 9.00 pm
Google



Mission is critical for driving other elements that we need to run the business


Strategic Intent
A declaration of an ambition that concretely describes the desired end-state.
"How will we know when we are done?"
See go/strategic-intent for a more detailed explanation of strategic intent.

Which one do you think is better?

"Develop digital readiness for the transformation of the 21st Century to modernize Britain and create a more digitally-literate country."

Or

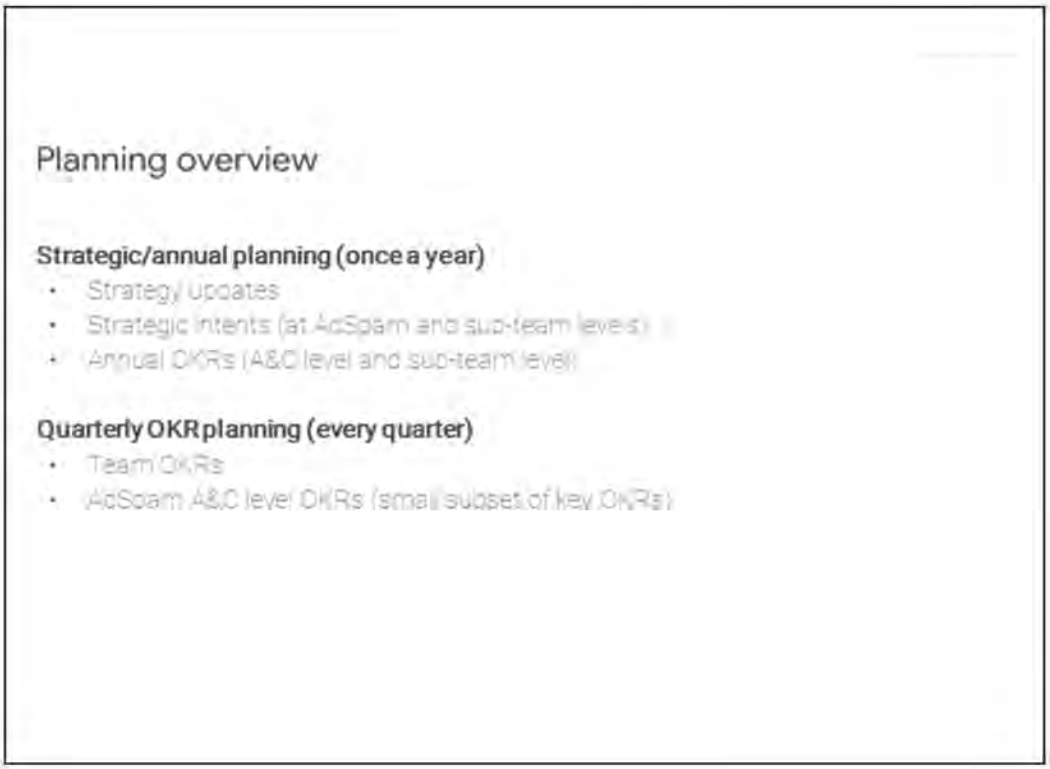
"To get everyone in the U.K. online by the end of 2012."

- Martha Lane Fox, Appointed as UK's Digital Champion

Example: AdSpam Sales Enablement

100% of our sales (and support) teams are ***autonomously*** able to communicate our AdSpam efforts with anyone, anywhere, anytime.

Put differently: zero inbound requests to AdSpam Advocacy XFN team for individual help discussing ad fraud with customers.



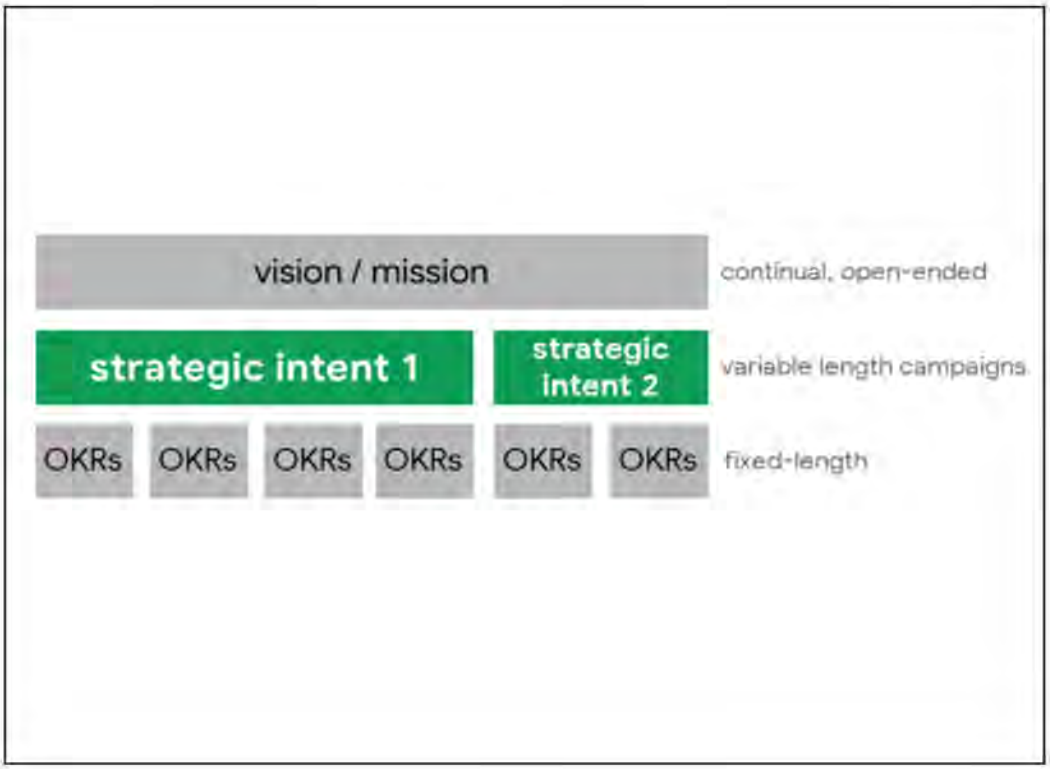
Strategy updates are directional
Strategic intent is more open ended (can span multiple years)
Annual OKRs are more specific and time-bound?

"Half year OKR planning"

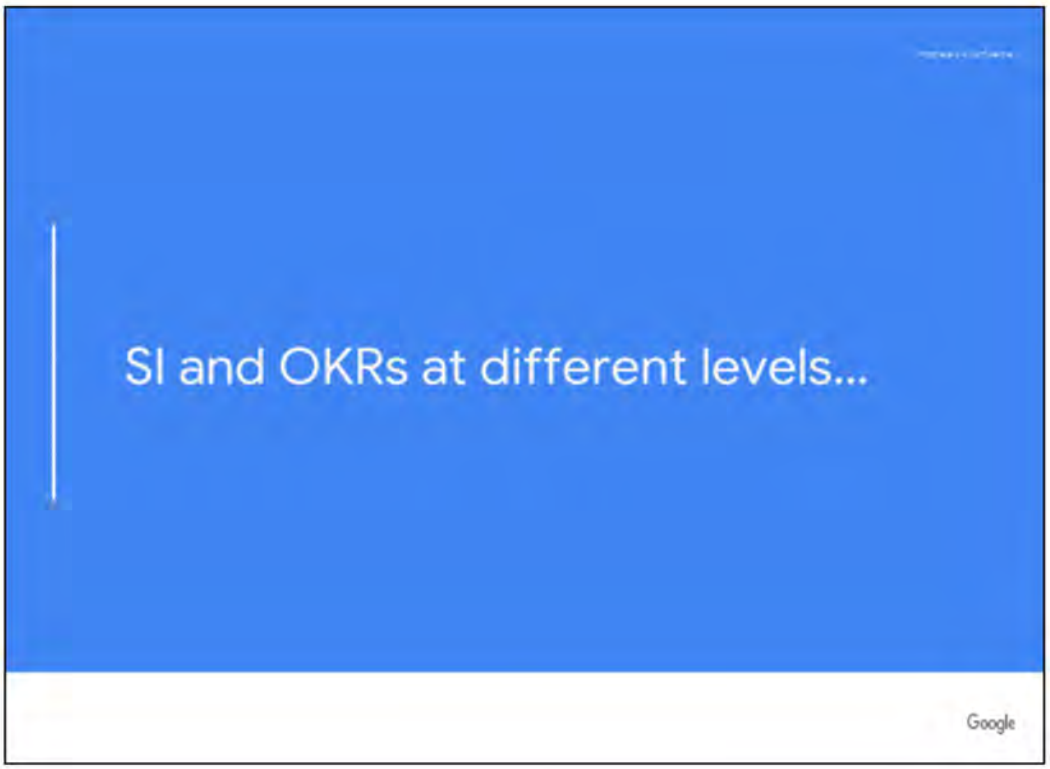
Suggested: Partially follow a "half-year planning" approach

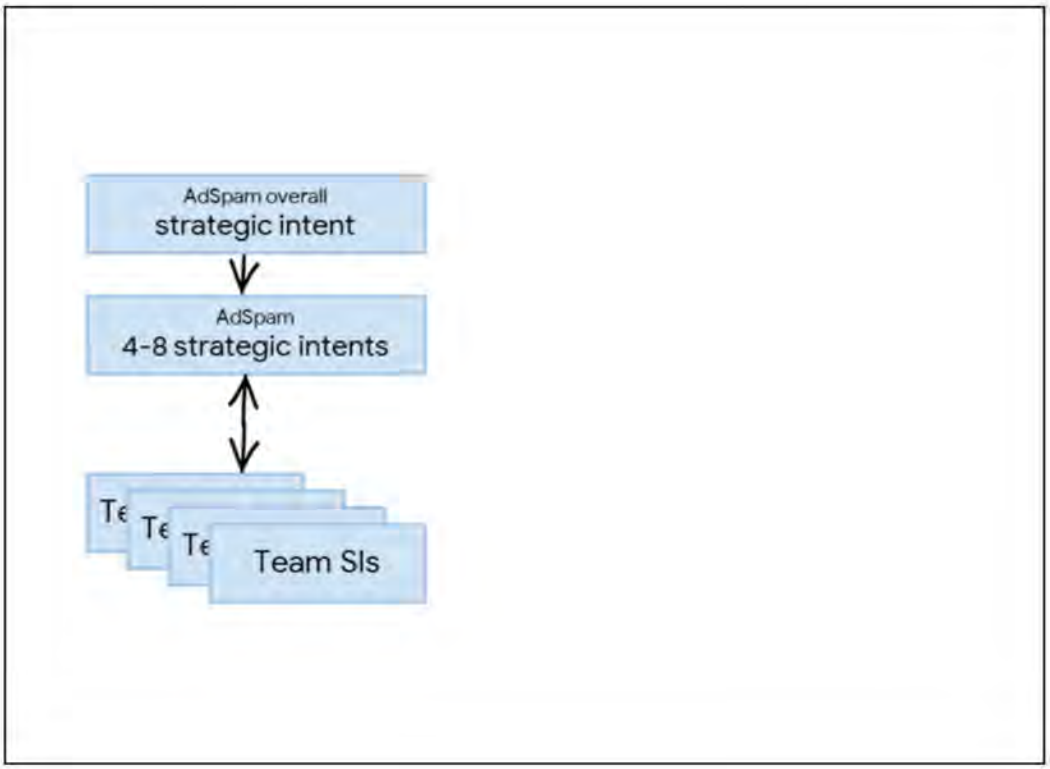
- Half-year (6 months) planning tasks (in Nov/Dec for H1, in June for H2)
  - Gather input from and align with stakeholders
  - Review new trends/strategic changes/etc
  - Stack-rank projects
- Every quarter planning tasks: "official quarterly OKR planning"
  - Estimate efforts
  - Assign resources
  - Above/below the line decisions
  - Enter into EasyOKR etc

Goal is to reduce the planning overhead in a pragmatic way

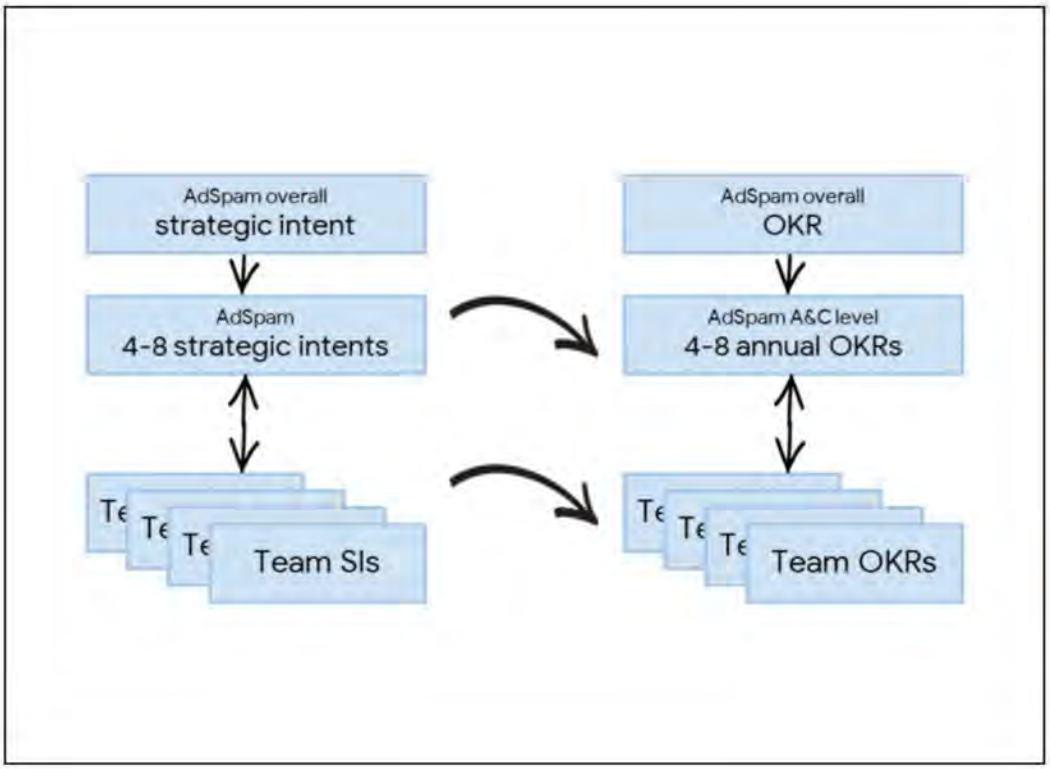


Speaker: Per
While quarterly OKRs are a great way of planning near-term work, the OKRs approach tends to fall short when it comes to strategic planning and management. Why? → Because OKRs are bound to arbitrary durations of time. As a result, teams, organizations, and PAs may find themselves optimizing for the short-term.


SI and OKRs at different levels...
Google

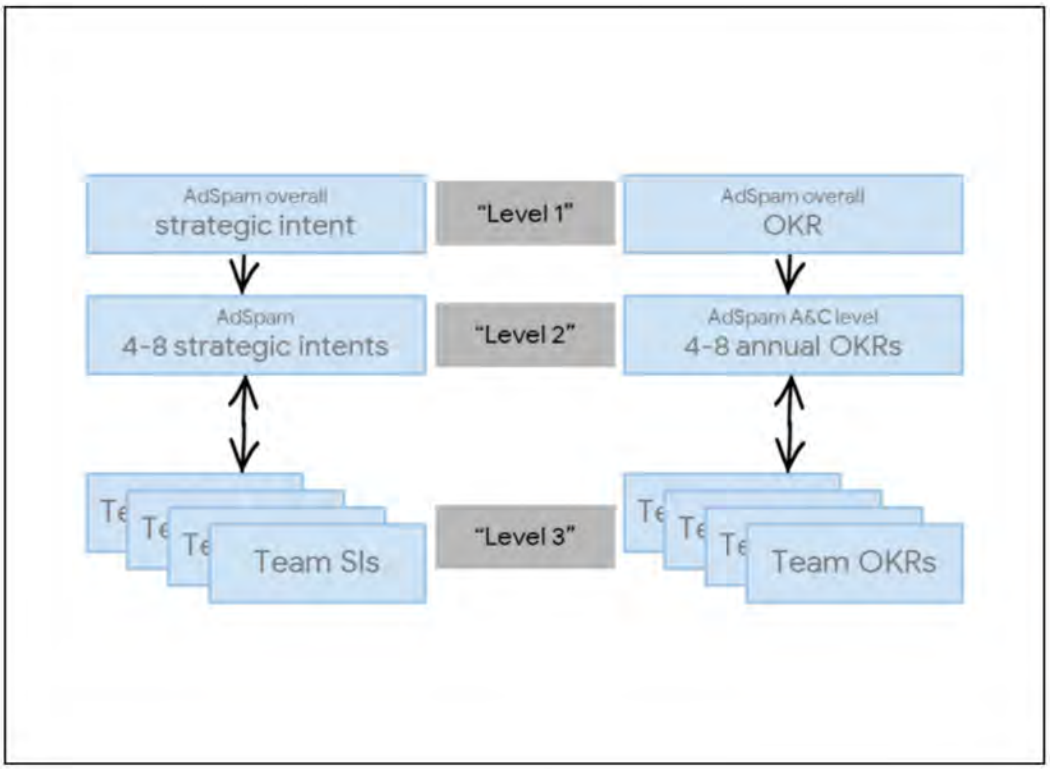

AdSpam overall
strategic intent
AdSpam
4-8 strategic intents
Te
Te
Te
Team SIs

Speaker: Per

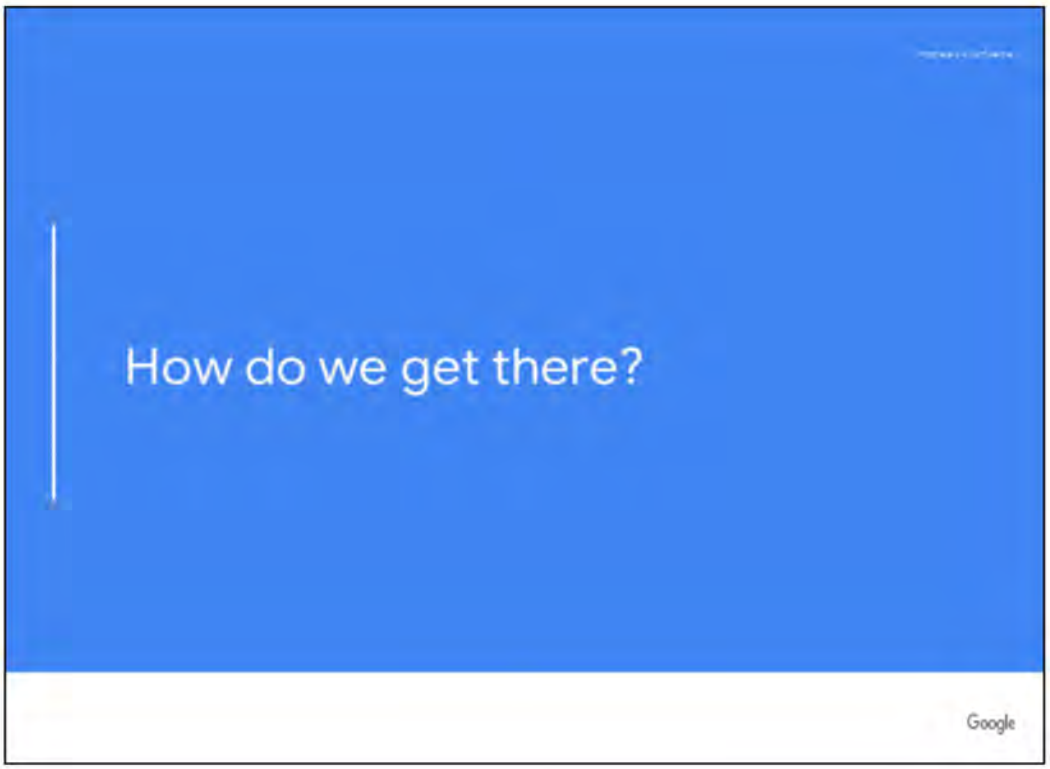


Speaker: Per
Strategic intents inform/drive OKRs
OKRs lead teams to realize a strategic intent.

Id	Date	Text
1	06/23/2020 08:45:48	+bjorke@google.com flagging that the relationship should be called out wrt to the Strategic Intents and how they inform/drive the OKRs. Maybe do so verbally or add some text to the arrows. The key point to drive home is that the OKRs lead teams to realize a strategic intent, and not vice versa.

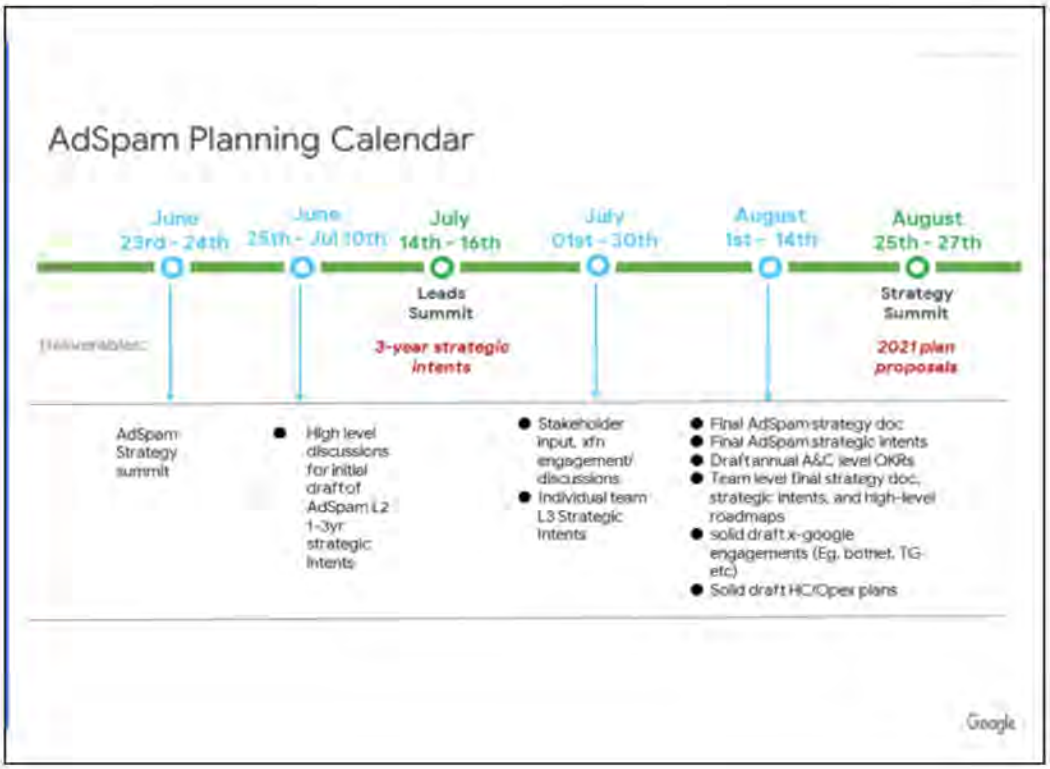

AdSpam overall
strategic intent
"Level 1"
AdSpam overall
OKR
AdSpam
4-8 strategic intents
"Level 2"
AdSpam A&C level
4-8 annual OKRs
Team SIs
"Level 3"
Team OKRs

Speaker: Per


How do we get there?
Google

Speaker: Aruna

Id	Date	Text
2	06/23/2020 14:44:17	+bjorke@google.com Small nit: Let's rephrase as high-level strategic intents instead of 3-year strategic intents.
1	06/23/2020 14:44:17	This is APaS level slide as it is. The guidance is for 3 years



Speaker: Aruna

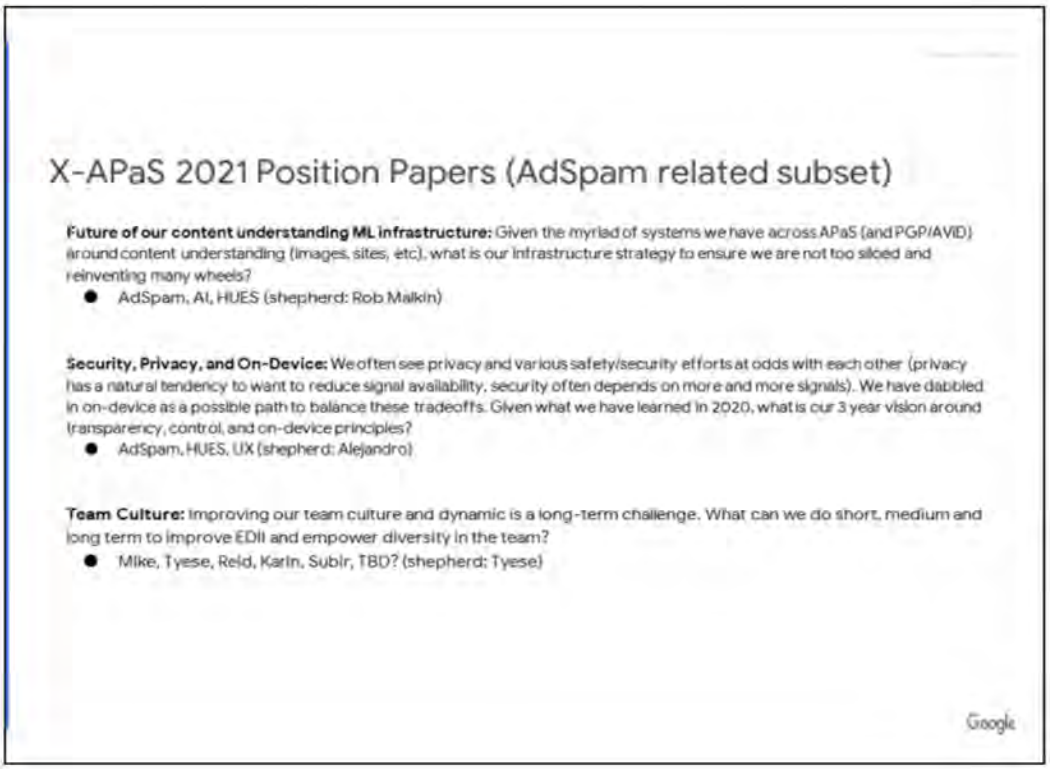
APaS Slides: https://docs.google.com/presentation/d/1N_D989fGKpVq1cuN0UEtFi-EhzgXmyZbxyTLI5kQD4k/edit#slide=id.g5d3751fd3e_3_53

Draft AdSpam strategy doc
July 14:
Solid draft AdSpam strategic intents (4-7 overall SIs; not sub-team specific)
Team: draft strategy doc, strategic intents (2-5 per team), and high-level roadmap
June/July: Stakeholder input, xfn engagement/discussions, etc.
Aug 25:
Final AdSpam strategy doc
Final AdSpam strategic intents
Draft annual A&C level OKRs
Team level final strategy doc, strategic intents, and high-level roadmaps
solid draft x-google engagements (Eg. botnet, TG etc)
solid draft HC/Opex plans
Nov/Dec:
Finalize annual A&C level OKRs (5-8 OKRs)
Q1 OKR planning
Separately: Q3 OKRs

Leads summit
3-year strategic intents
Full doc for pre-read
1-3 slides to guide presentation
X-APaS position papers
1-3 slides to solicit input
No doc due for 7/14-16

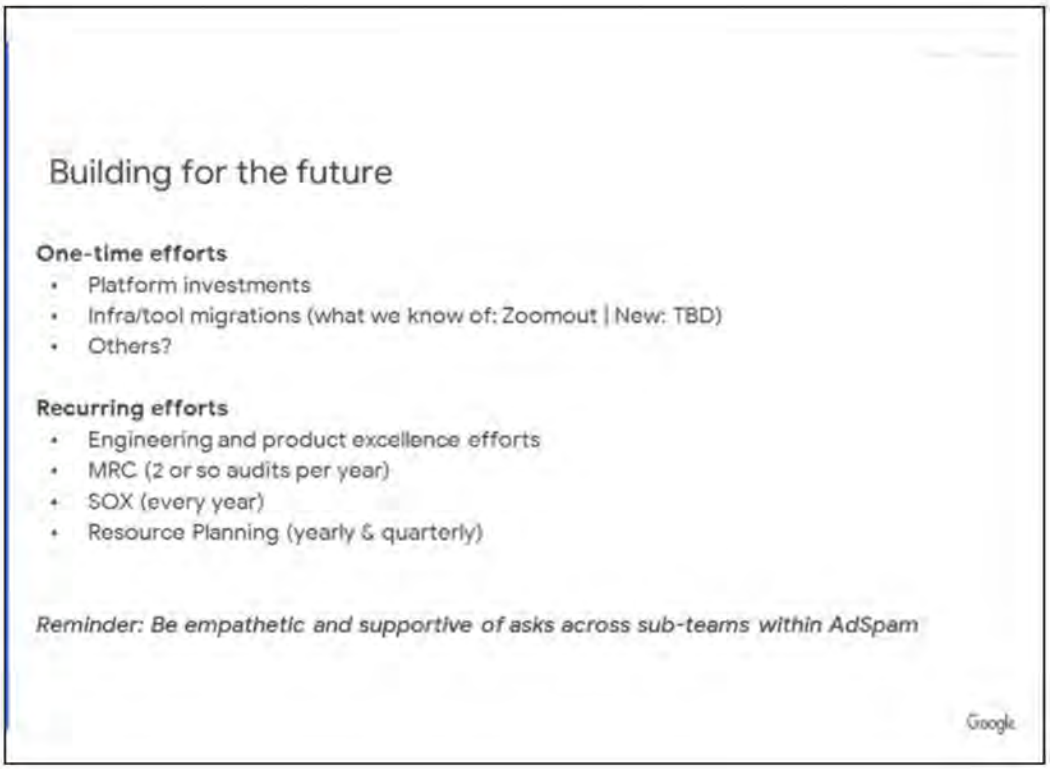
Strategy summit
2021 plan proposals
Full doc (draft OKRs, project prioritization, HC / OpEx ask, X-google engagement plans, etc.)
1-3 slides to guide presentation
Final X-APaS position papers
Full doc for pre-read
1-3 slides to guide presentation
Note: full X-APaS position papers are due 8/3, but will be shared / iterated up to the strategy summit

Id	Date	Text
3	06/23/2020 09:25:50	+bjorke@google.com same here. Suggest striking 3yr from strategic intents (we don't want to frame as time-bound?)

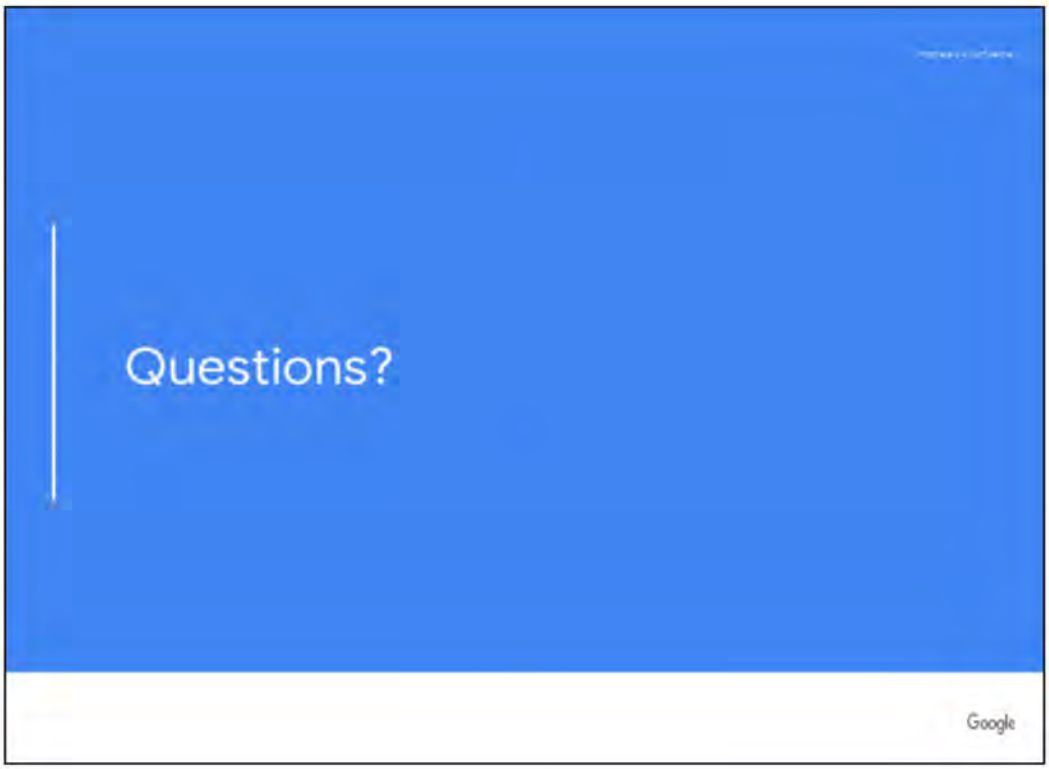


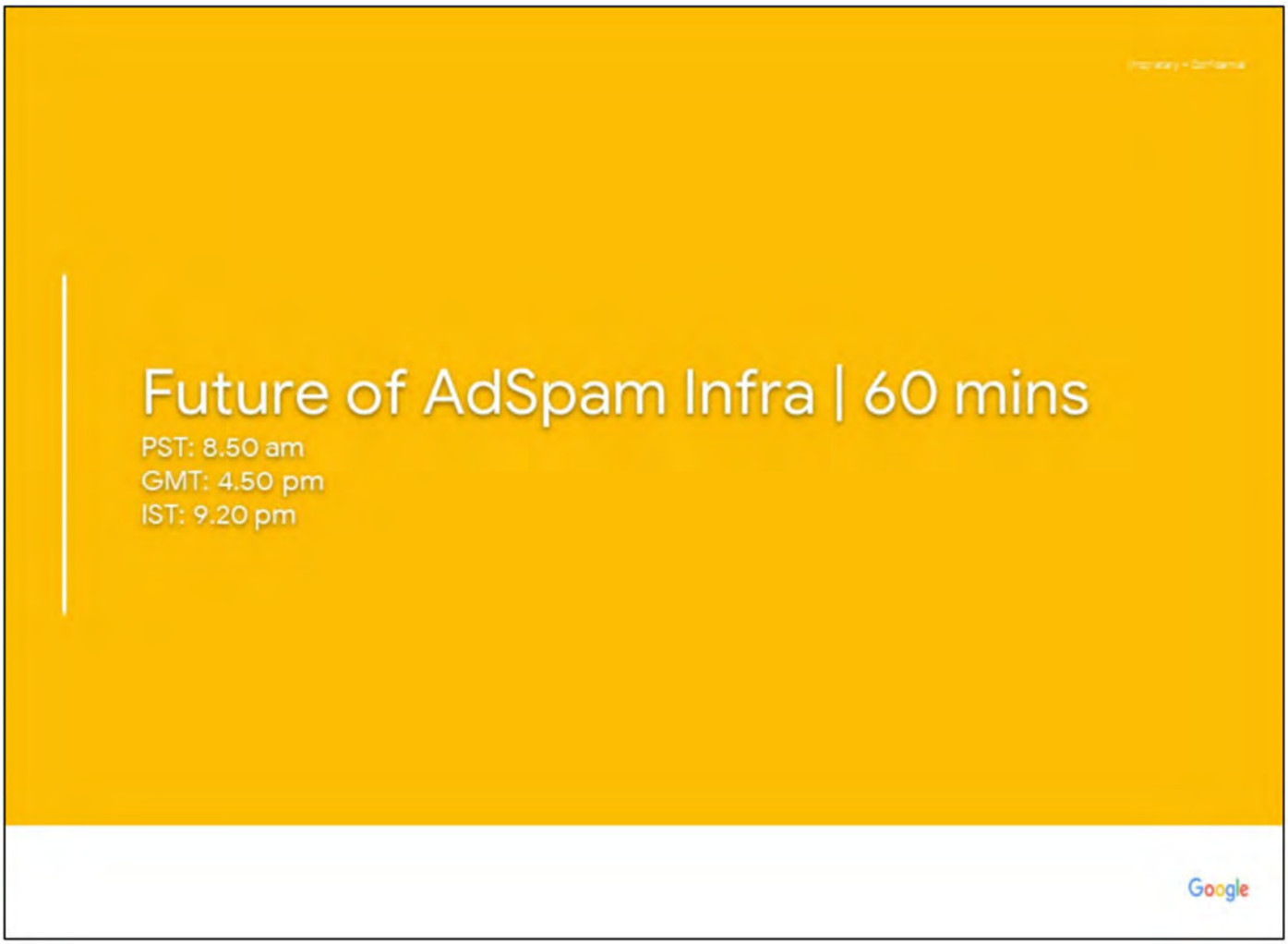
Speaker: Aruna

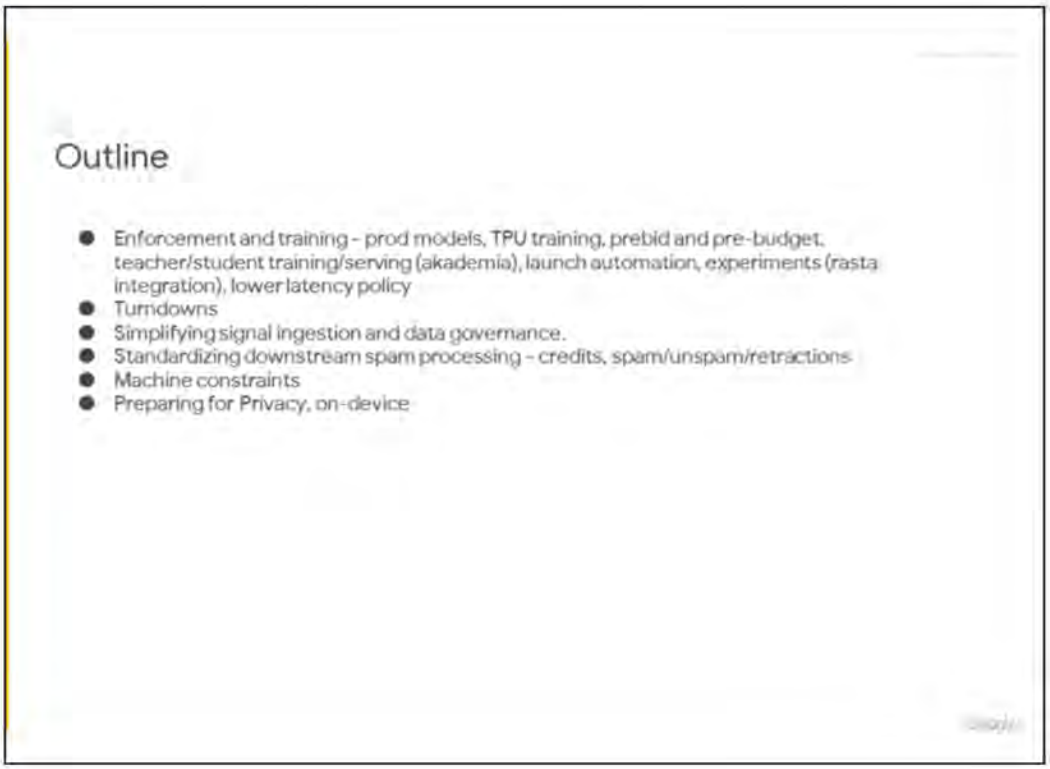
Id	Date	Text
1	06/23/2020 23:49:35	@aruna@google.com What's Alejandro's ldap? Should we be engaging with the on-device x-apas 2021 position paper? _Reassigned to Aruna Kommu_
2	06/23/2020 23:49:35	aborgia , FYI, Subir mentioned in the summit that he will connect the right group to Alejandro.

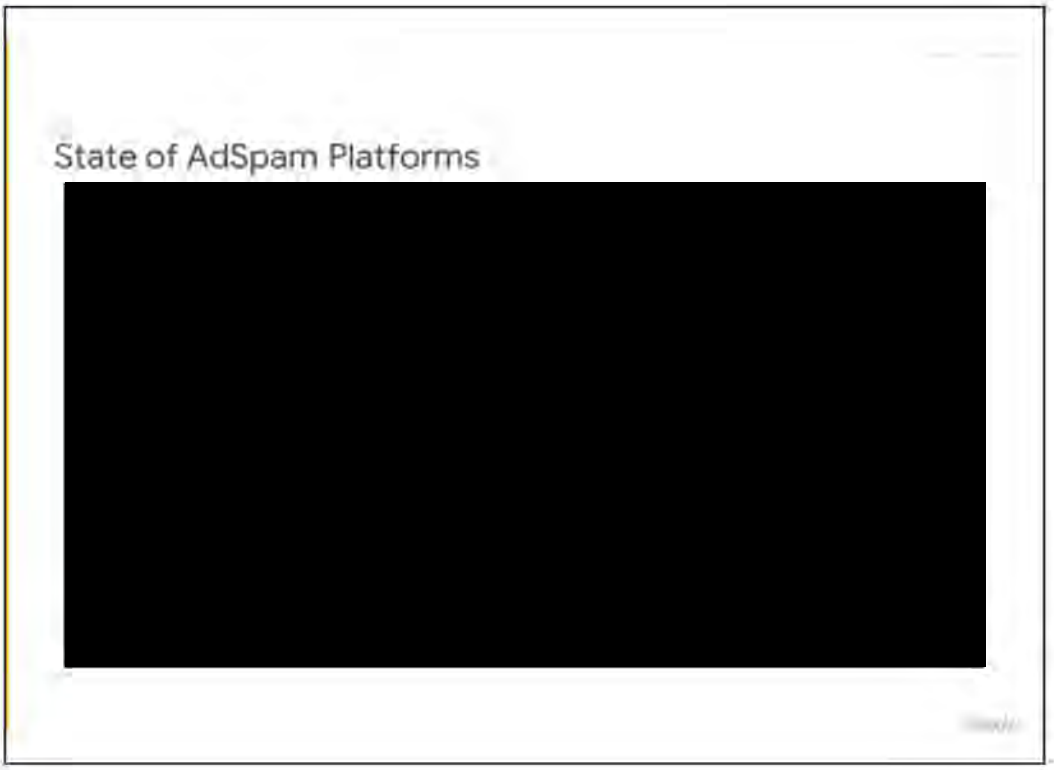


Speaker: Aruna

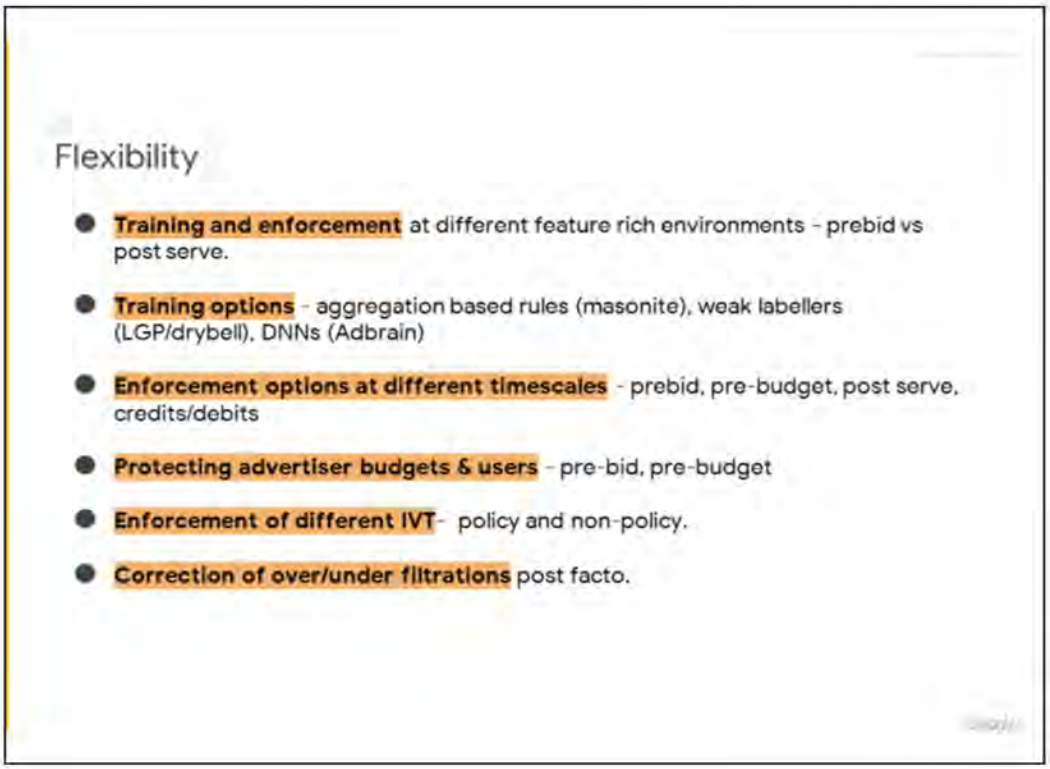

Questions?
Google


Future of AdSpam Infra | 60 mins
PST: 8.50 am
GMT: 4.50 pm
IST: 9.20 pm
Google

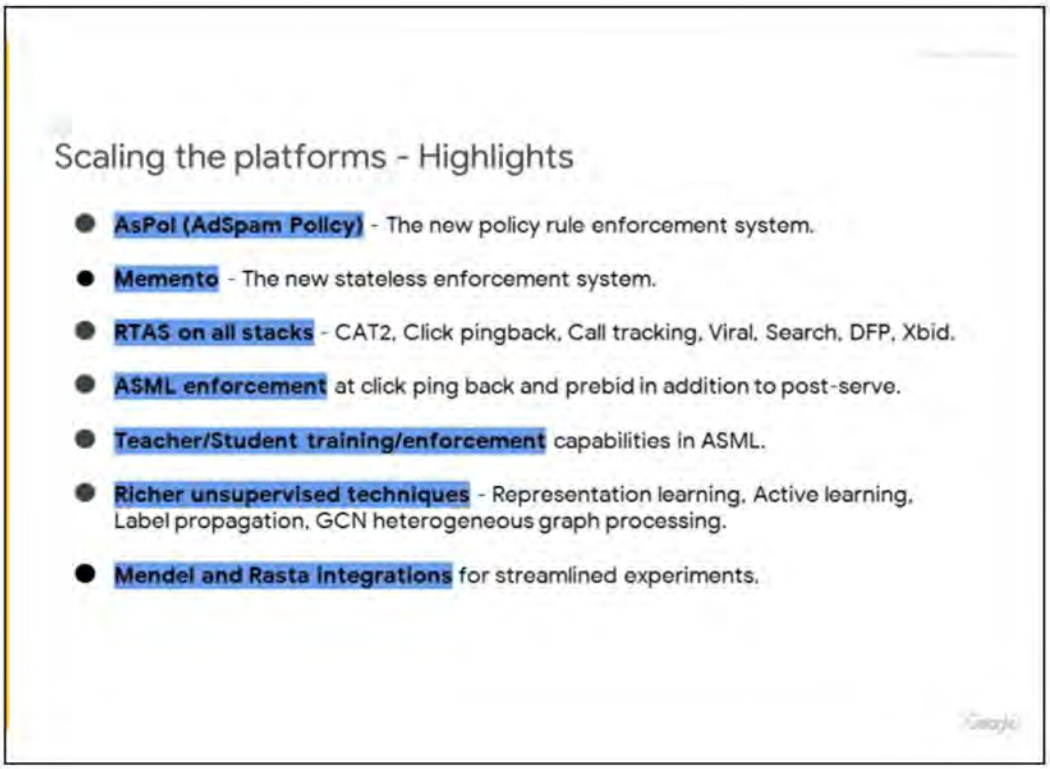

Outline
Enforcement and training - prod models, TPU training, prebid and pre-budget, teacher/student training/serving (akademia), launch automation, experiments (rasta integration), lower latency policy
Turndowns
Simplifying signal ingestion and data governance.
Standardizing downstream spam processing - credits, spam/unspam/retractions
Machine constraints
Preparing for Privacy, on-device



Famous picture that we use to scare Nooglers in AdSpam. At times this has also helped in convincing senior leadership to do some painful investments.
But instead of focusing on the complexity I want to emphasize the strengths.



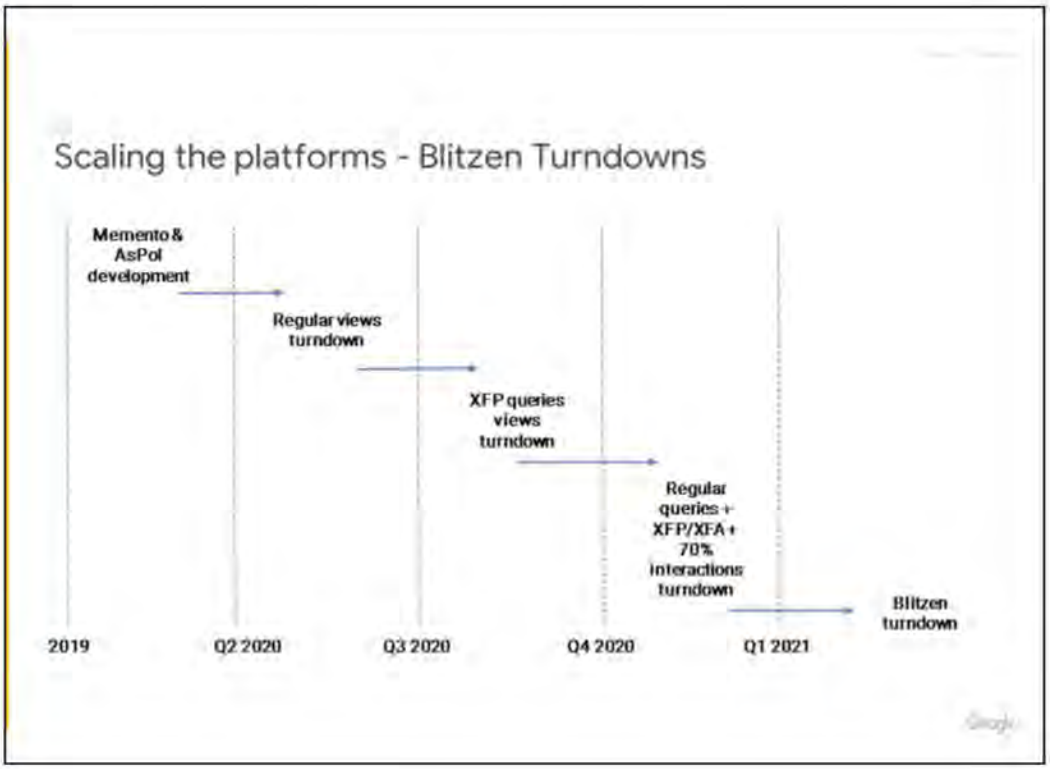
Biggest strength is flexibility.
Training & enforcement - joined logs vs just the bare QEM or just the bare CEM
Enforcement options at different timescales - different options have different impact on the business and our advertisers; These also come with tradeoffs around what you can train with.
Protecting advertiser budgets & users against different kinds of spam



AsPol - streaming grouping and aggregation

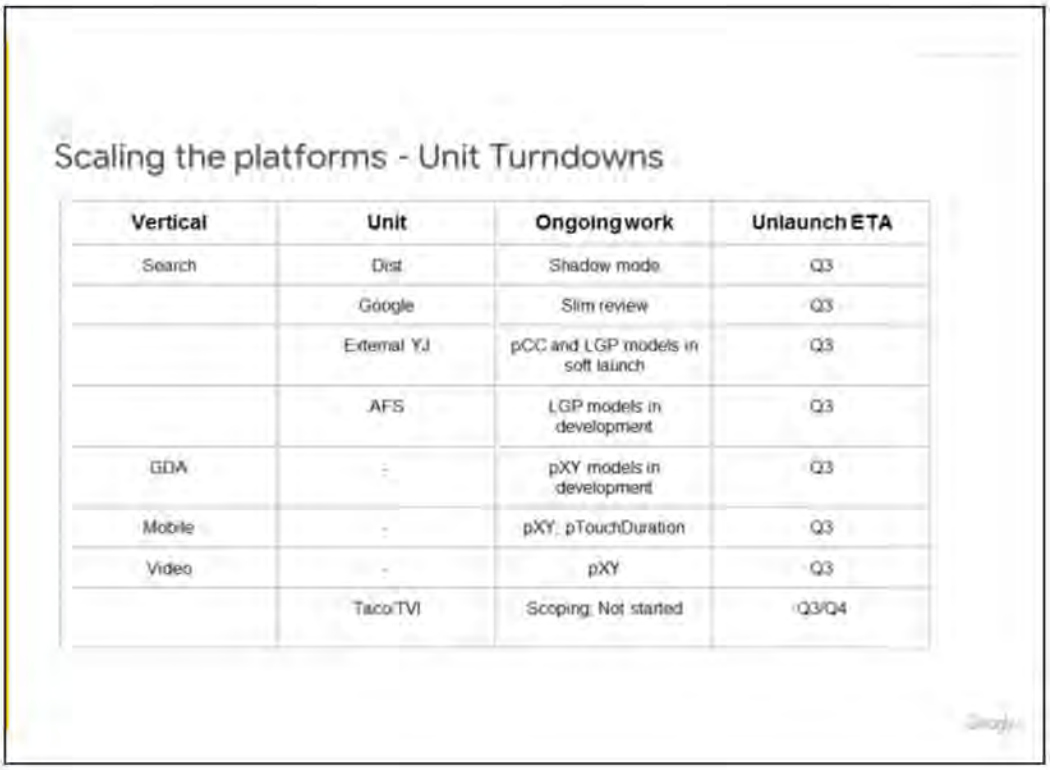
One of the ways in which we are trying to tackle these challenges is by putting more wood behind fewer arrows and limiting our focus on fewer systems - systems that cover all use cases (policy, non-policy, different enforcement options, different training options) which are built on modern sustainable architectures and technology.

To that end we have an A&c level goal to turn down blitzen which happens to be one of the largest and complicated system in our fleet. Back in 2018 we did a CM that stabilized Blitzen but the cracks are again beginning to show.



Challenges:
- Blitzen non-determinism
- Blitzen lack of past spam capabilities
- No portability
- Incre/decre cannot be measured with metrics

Id	Date	Text
1	06/23/2020 12:08:41	@jfmatthews@google.com @vram@google.com sgty?
1	06/23/2020 12:08:41	Q4 seems very crammed given that its a short quarter. XFP/XFA = 7 pipelines (given that xfp views should get done in Q3).



Scaling the platforms - Unit Turndowns

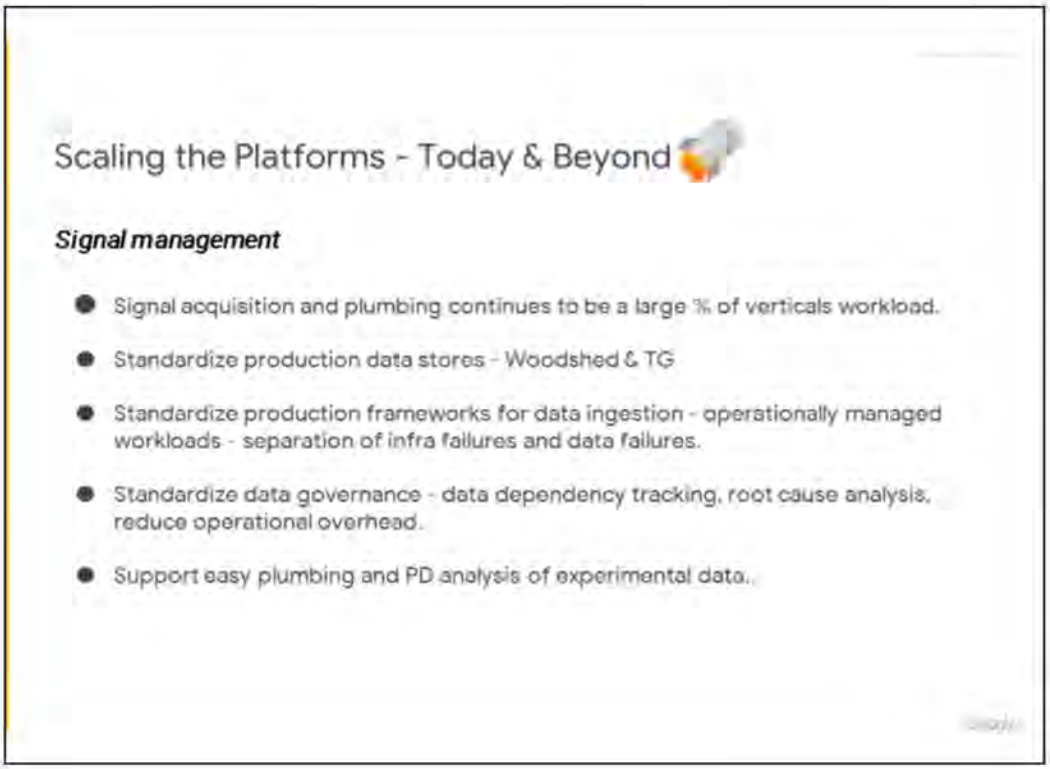
Vertical	Unit	Ongoing work	Unlaunch ETA
Search	Dist	Shadow mode	Q3
	Google	Slim review	Q3
	External YJ	pCC and LGP models in soft launch	Q3
	AFS	LGP models in development	Q3
GDA	-	pXY models in development	Q3
Mobile	-	pXY; pTouchDuration	Q3
Video	-	pXY	Q3
	Taco/TVI	Scoping; Not started	Q3/Q4

- Largely making good progress; search &gda -- well defended on asml; mobile & video - pxy;
- unlaunches are followed by shadow mode experiments for a quarter to study if the existing defenses are helping capture a unique fingerprint of spam.

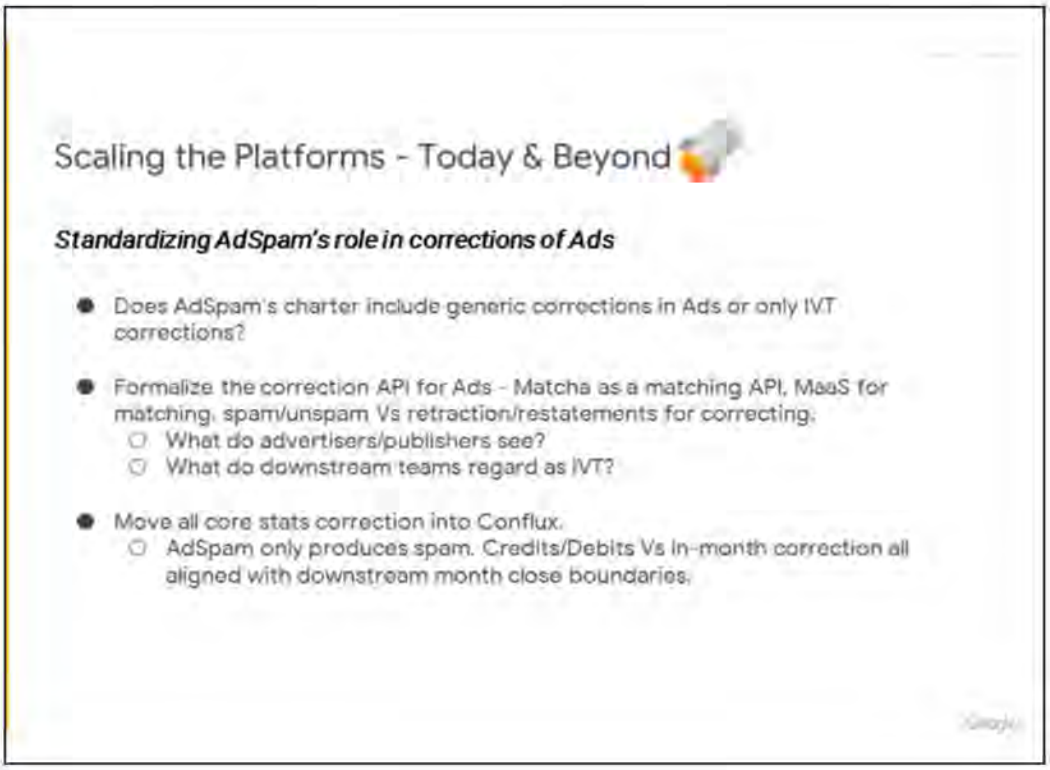
- Shoutout to verticals and TnS - Cross team effort to streamline our defenses and simplify our systems.

- So this is today and how we are walking down the path that we set out in 2018/2019. But whats in store for the future. Beyond stabilizing and simplification we want to invest in areas that can increase AdSpam's impact and improve productivity.

Id	Date	Text
2	06/23/2020 16:47:44	@kendrickb@google.com @jfmatthews@google.com does this look fine. I tried to compile info from the status spreadsheet and Kendrick's doc.
1	06/23/2020 16:47:44	For Afs, something like "sprint to develop PCC and LGP models in July" is the current status. Video also has ongoing, required work to launch expanded PCC models.



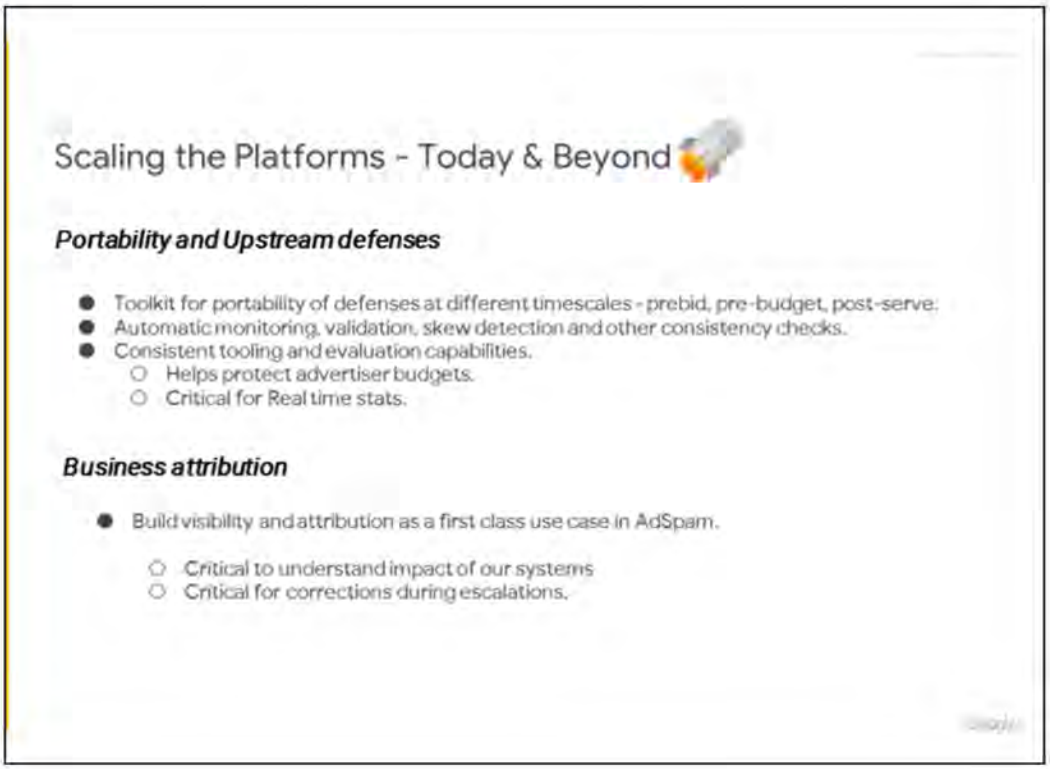
We want you to be able to not worry about how the data is sourced; you should be responsible for validation of sanity of data and the business logic that makes use of this data but everything else should be automated for you.

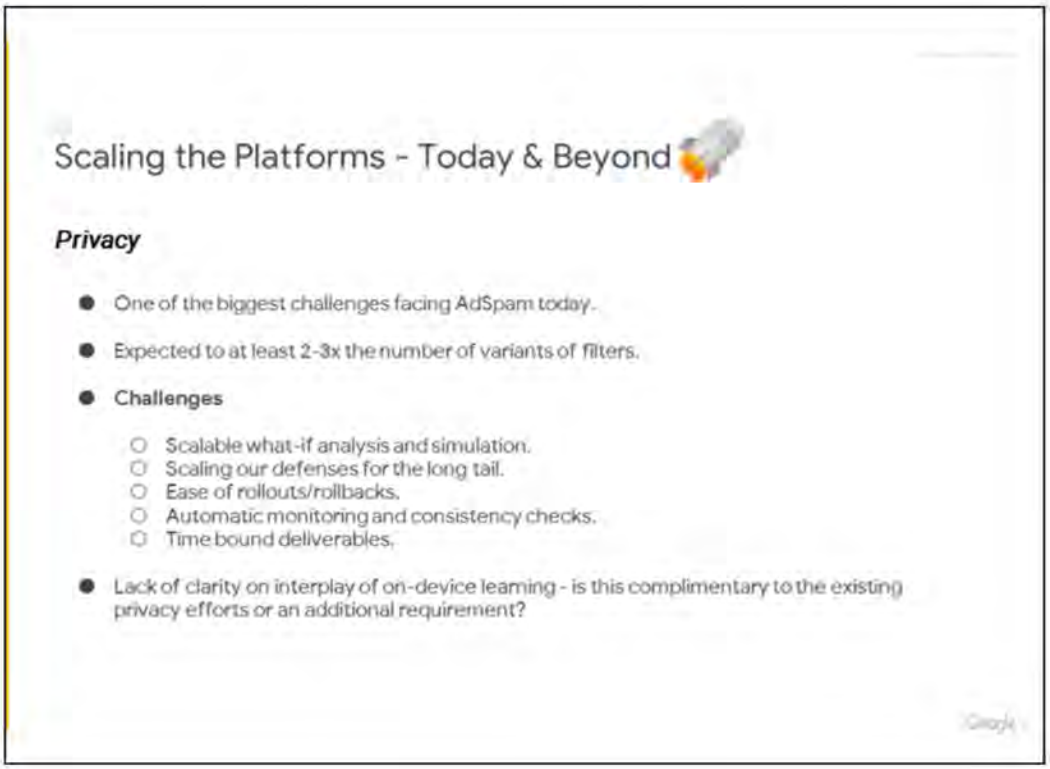


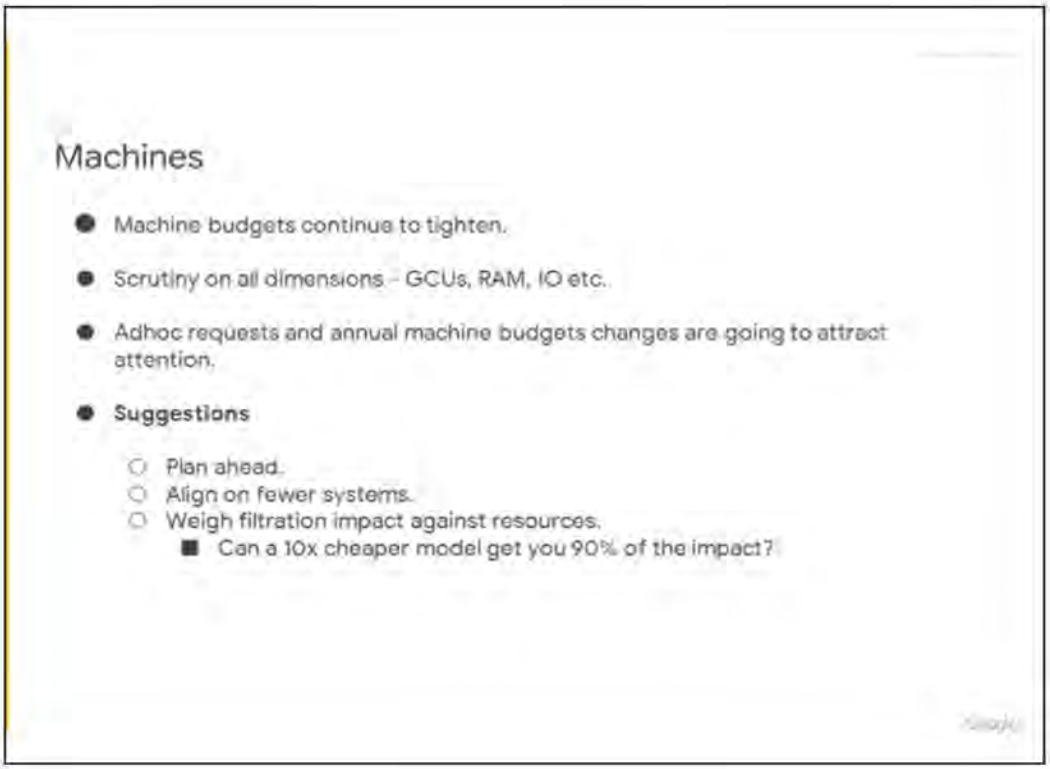
This is a broad area that goes beyond Adspam but it is very relevant for our day to day operations. AdSpam is in the business of identify and enforcing IVT - both policy and non-policy. But there have been several incidents in the past where AdSpam annotations are used for correcting experiments that have gone wrong. There are new use cases emerging where Ads looks at AdSpam as a way to correct stats/advertiser payouts.

There are several reasons for this - we have a popular set of APIs and services for picking the relevant events that need to be corrected and we have the systems to produce the annotations that have the intended impact. But are these the correction annotations?

Beyond standardizing and clarifying our role we also want separation of concerns - AdSpam should not be in the business of monetizating IVT/correctons - not an area where our strengths are and we are not properly setup to handle this charter.

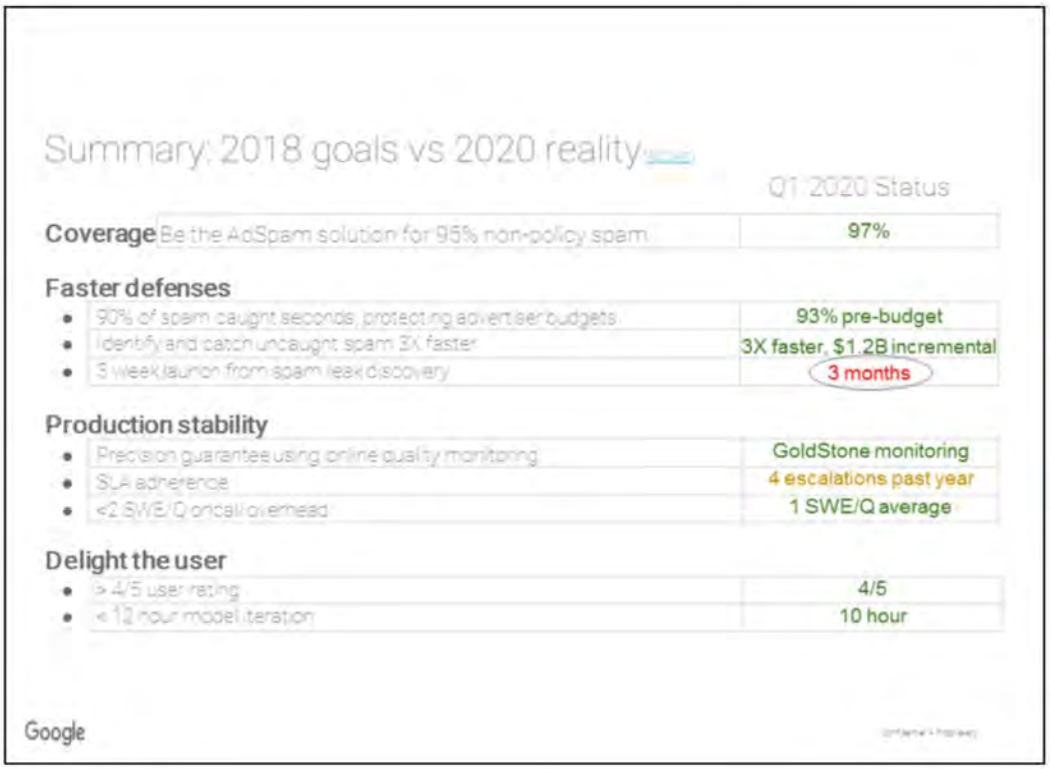

Scaling the Platforms - Today & Beyond
Portability and Upstream defenses
Toolkit for portability of defenses at different timescales - prebid, pre-budget, post-serve.
Automatic monitoring, validation, skew detection and other consistency checks.
Consistent tooling and evaluation capabilities.
Helps protect advertiser budgets.
Critical for Real time stats.
Business attribution
Build visibility and attribution as a first class use case in AdSpam.
Critical to understand impact of our systems
Critical for corrections during escalations.


Scaling the Platforms - Today & Beyond
Privacy
One of the biggest challenges facing AdSpam today.
Expected to at least 2-3x the number of variants of filters.
Challenges
Scalable what-if analysis and simulation.
Scaling our defenses for the long tail.
Ease of rollouts/rollbacks.
Automatic monitoring and consistency checks.
Time bound deliverables.
Lack of clarity on interplay of on-device learning - is this complimentary to the existing privacy efforts or an additional requirement?



And lastly a word from our sponsors - capital engineering

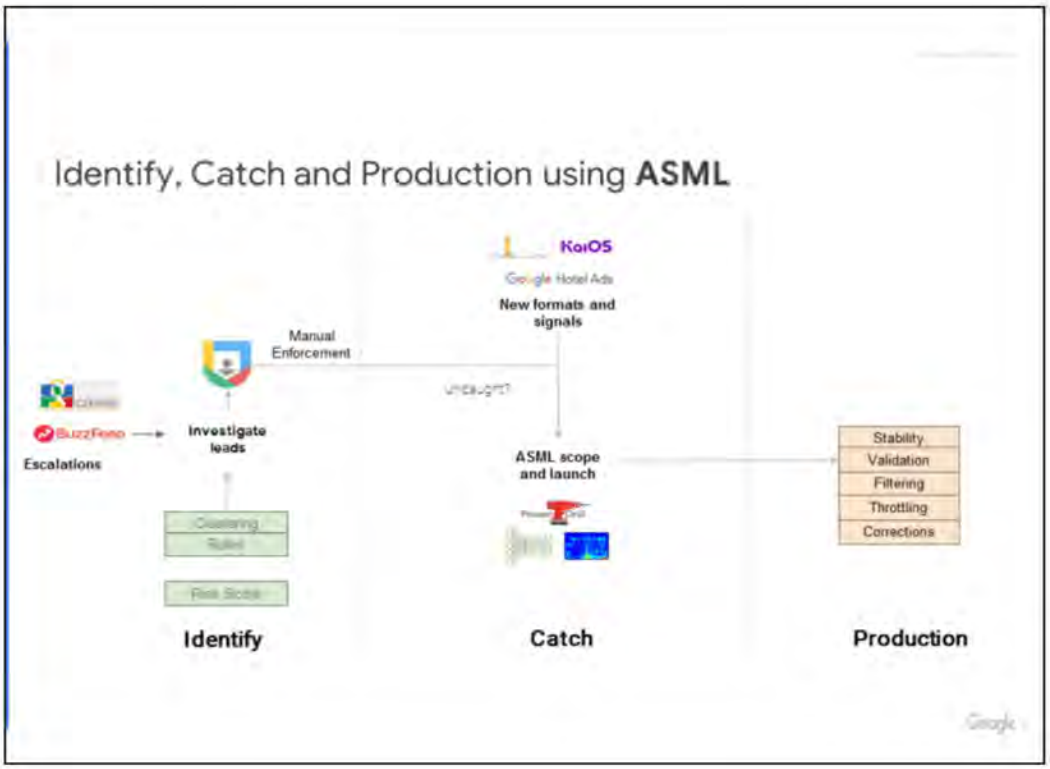
Ex. display doesn't serve the entire corpus of 300+M ads - only 20M at any time.

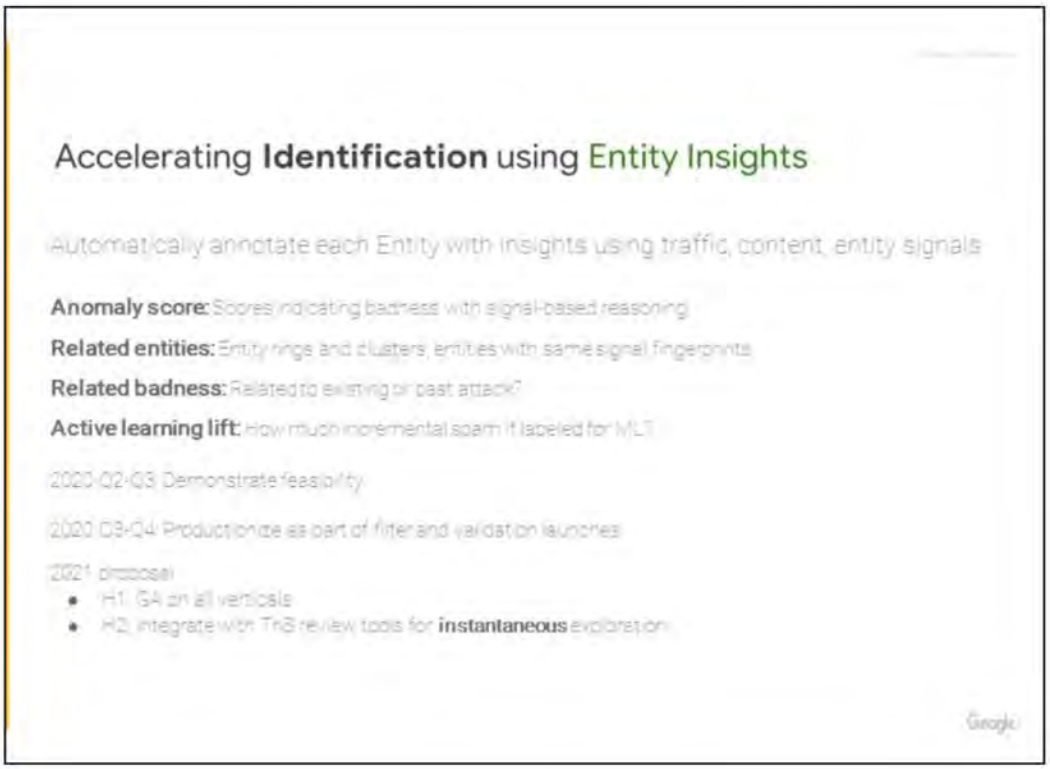


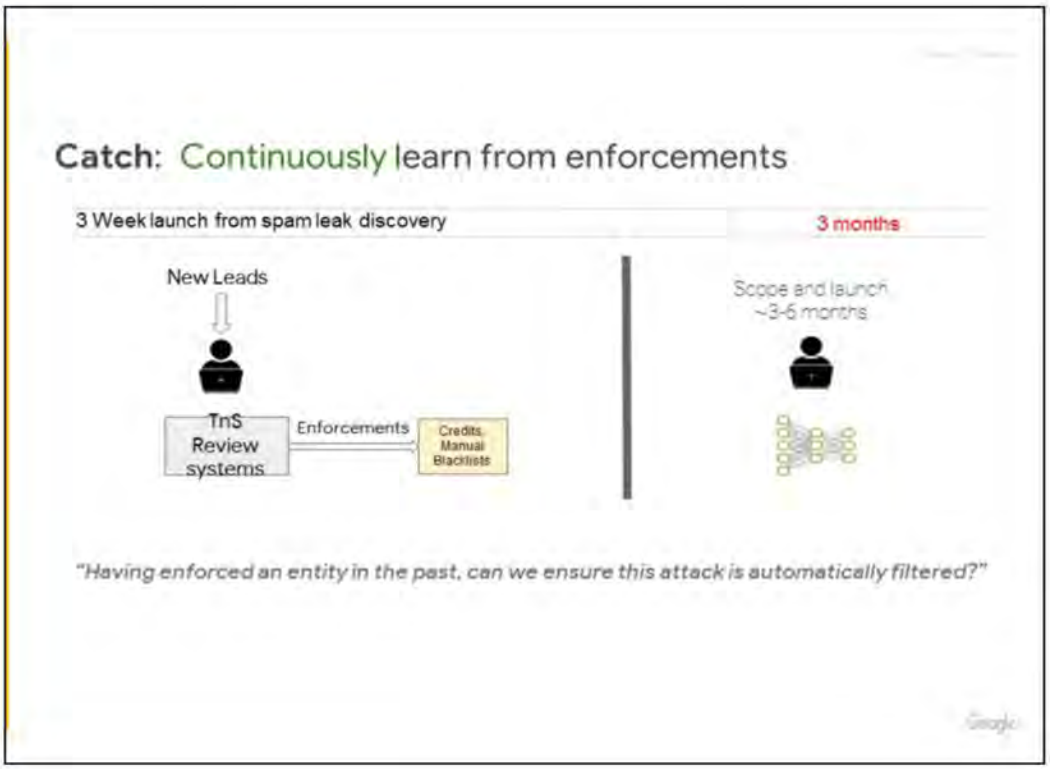
Summary: 2018 goals vs 2020 reality

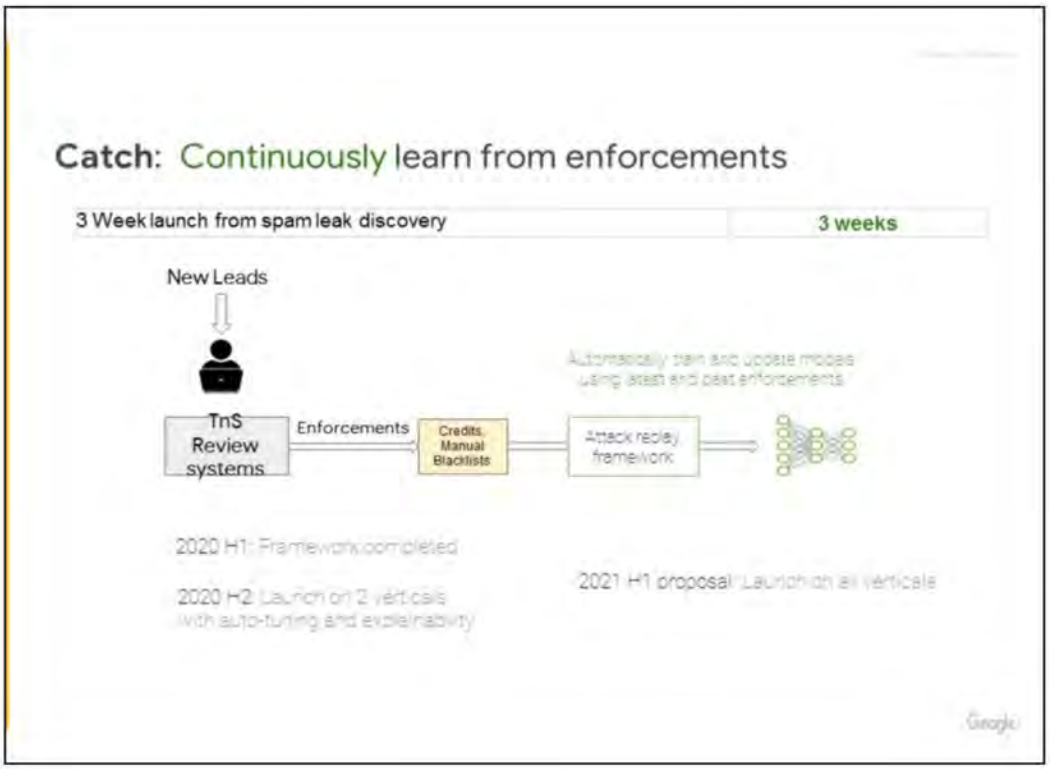
		Q1 2020 Status
Coverage	Be the AdSpam solution for 95% non-policy spam	97%
Faster defenses		
•	90% of spam caught seconds, protecting advertiser budgets	93% pre-budget
•	Identify and catch uncaught spam 3X faster	3X faster, $1.2B incremental
•	3 week launch from spam leak discovery	3 months
Production stability		
•	Precision guarantee using online quality monitoring	GoldStone monitoring
•	SLA adherence	4 escalations past year
•	<2 SWE/Q oncall overhead	1 SWE/Q average
Delight the user		
•	> 4/5 user rating	4/5
•	< 12 hour model iteration	10 hour

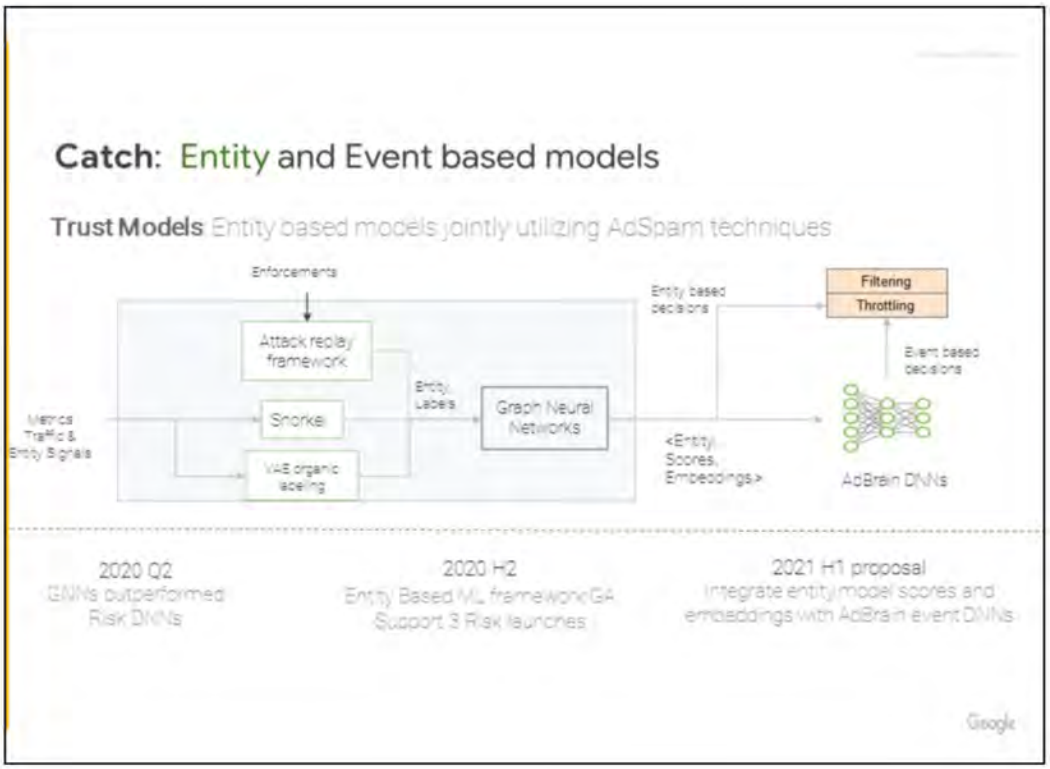
Google

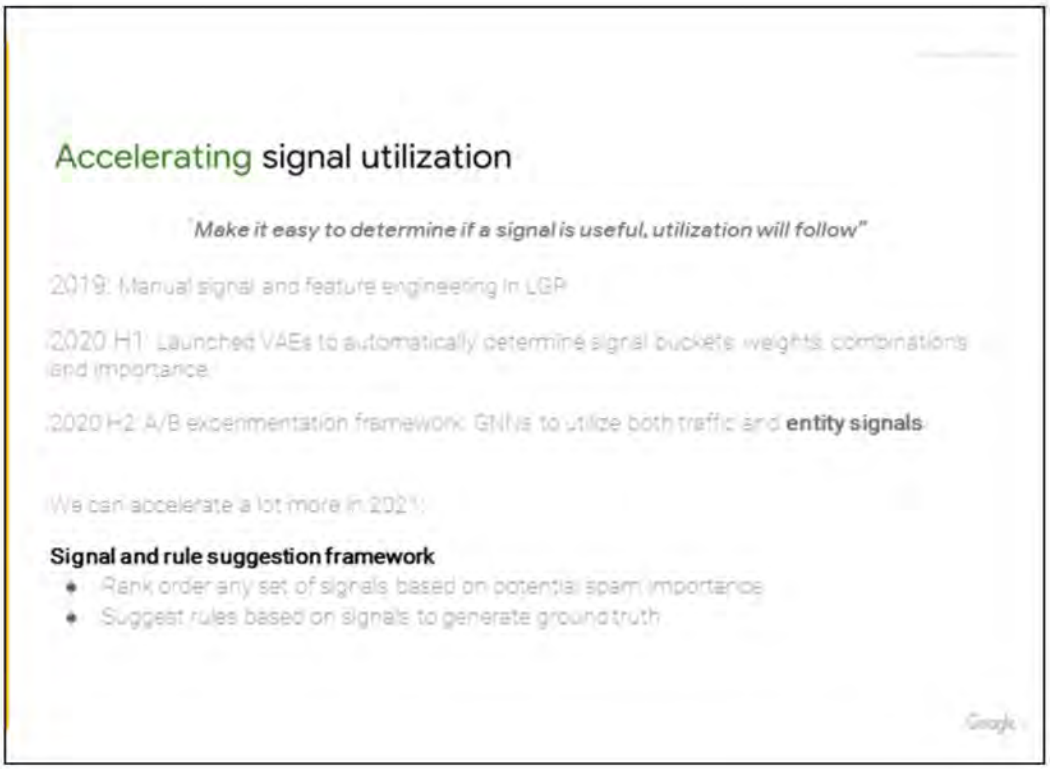

Identify, Catch and Production using ASML
KoiOS
New formats and signals
Manual Enforcement
Investigate leads
Escalations
ASML scope and launch
Stability
Validation
Filtering
Throttling
Corrections
Identify
Catch
Production


Accelerating Identification using Entity Insights
Automatically annotate each Entity with insights using traffic, content, entity signals
Anomaly score: Scores indicating badness with signal-based reasoning
Related entities: Entity rings and clusters, entities with same signal fingerprints
Related badness: Related to existing or past attack?
Active learning lift: How much incremental spam if labeled for MLT
2020 Q2-Q3: Demonstrate feasibility
2020 Q3-Q4: Productionize as part of filter and validation launches
2021 proposal:
H1: GA on all verticals
H2: integrate with TnS review tools for instantaneous evaluation
Google


Catch: Continuously learn from enforcements
3 Week launch from spam leak discovery
3 months
New Leads
TnS Review systems
Enforcements
Credits Manual Blacklists
Scope and launch ~3-6 months
"Having enforced an entity in the past, can we ensure this attack is automatically filtered?"


Catch: Continuously learn from enforcements
3 Week launch from spam leak discovery
3 weeks
New Leads
TnS Review systems
Enforcements
Credits, Manual Blacklists
Attack replay framework
2020 H1: Framework completed
2020 H2: Launch on 2 verticals with auto-tuning and explainability
2021 H1 proposal: Launch on all verticals
Google


Catch: Entity and Event based models
Trust Models Entity based models jointly utilizing AdSpam techniques
Enforcements
Attack replay framework
Snorkel
VAE organic labeling
Entity Labels
Graph Neural Networks
Entity based decisions
Filtering
Throttling
Event based decisions
<Entity Scores, Embeddings>
AdBrain DNNs
2020 Q2
GNNs outperformed Risk DNNs
2020 H2
Entity Based ML framework GA
Support 3 Risk launches
2021 H1 proposal
Integrate entity model scores and embeddings with AdBrain event DNNs
Google


Accelerating signal utilization
"Make it easy to determine if a signal is useful, utilization will follow"
2019: Manual signal and feature engineering in LGP
2020 H1: Launched VAEs to automatically determine signal buckets, weights, combinations and importance
2020 H2: A/B experimentation framework. GNN is to utilize both traffic and entity signals
We can accelerate a lot more in 2021:
Signal and rule suggestion framework
Rank order any set of signals based on potential spam importance
Suggest rules based on signals to generate ground truth
Google

Transfer learning

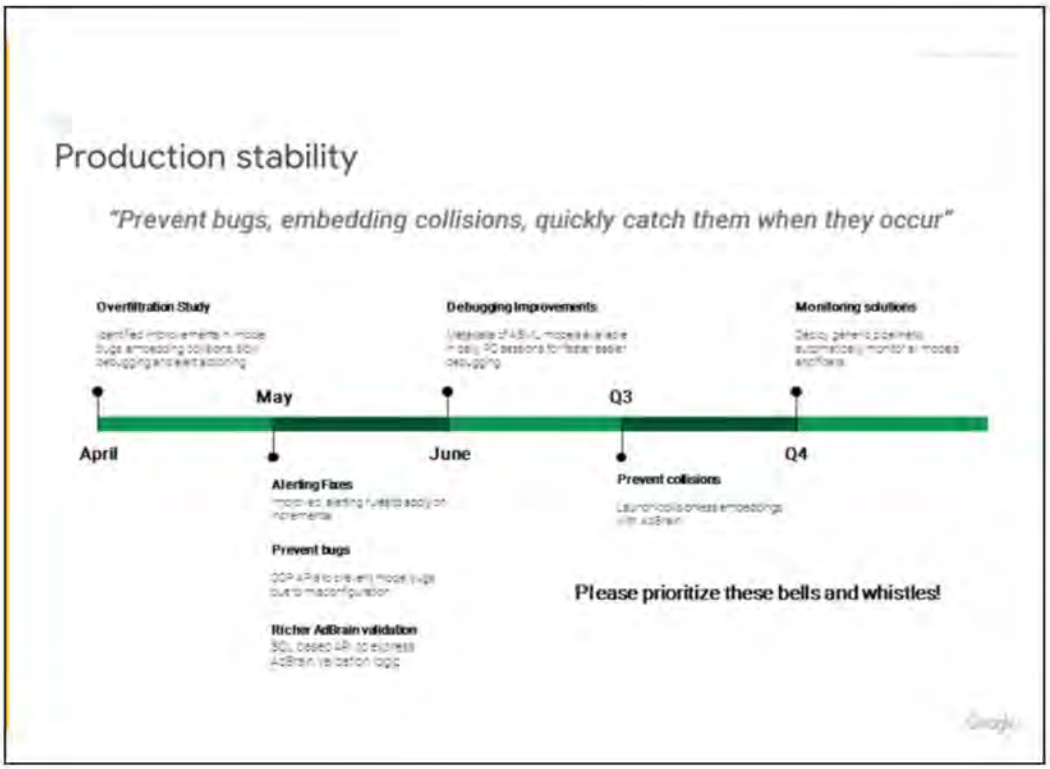
"Create large defenses in areas where signals or labels are lacking"

2020 H1
Transfer learning framework launched
GDA D2D, DCLK pre-bid scoped

2020 H2
Support Transfer learning launches for impression and pre-bid defenses

2021 proposal
Can we strengthen transfer learning to defend new formats, surfaces? Privacy-safe models?

Google


Production stability
"Prevent bugs, embedding collisions, quickly catch them when they occur"
Overfiltration Study
Debugging improvements
Monitoring solutions
April
May
June
Q3
Q4
Alerting Fixes
Prevent bugs
Prevent collisions
Richer AdBrain validation
Please prioritize these bells and whistles!

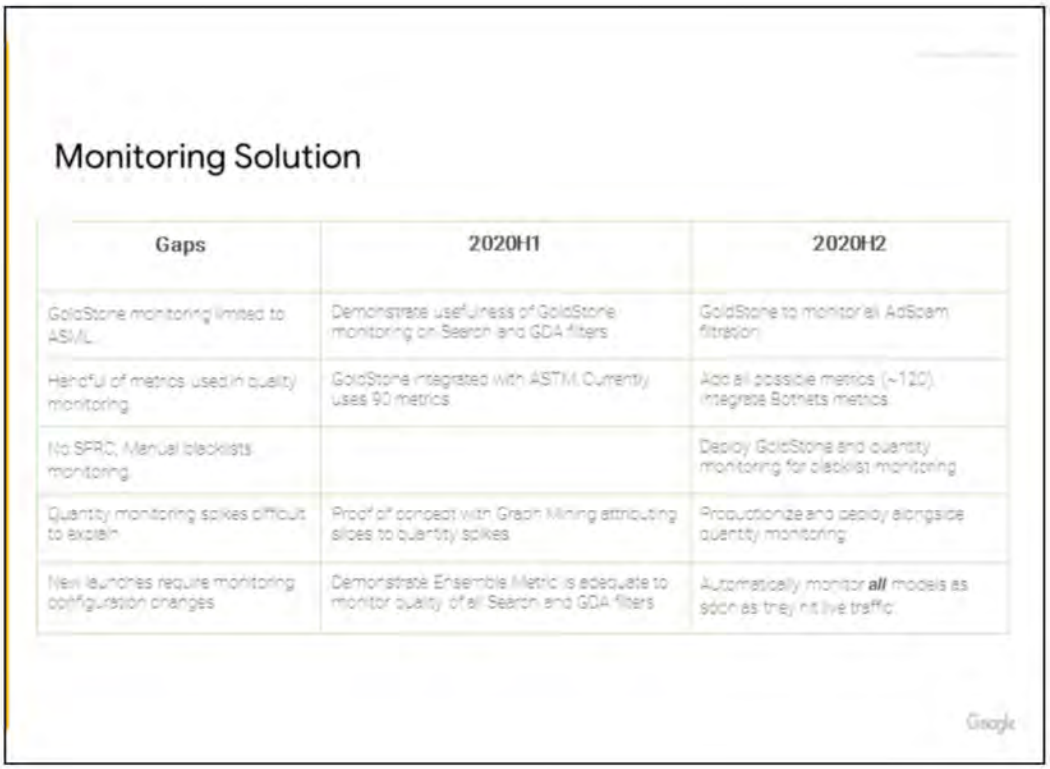
Monitoring Gaps

2019 Q4:

- GoldStone monitoring limited to ASM
- Handful of metrics used in quality monitoring
- No SFRC. Manual checklists monitoring
- Quantity monitoring covers only Boolean explain
- New launches require monitoring configured

2020 goal:

*"Any manual or automated filter is **automatically** quality and quantity monitored with slice-level attribution and 50% actionability"*

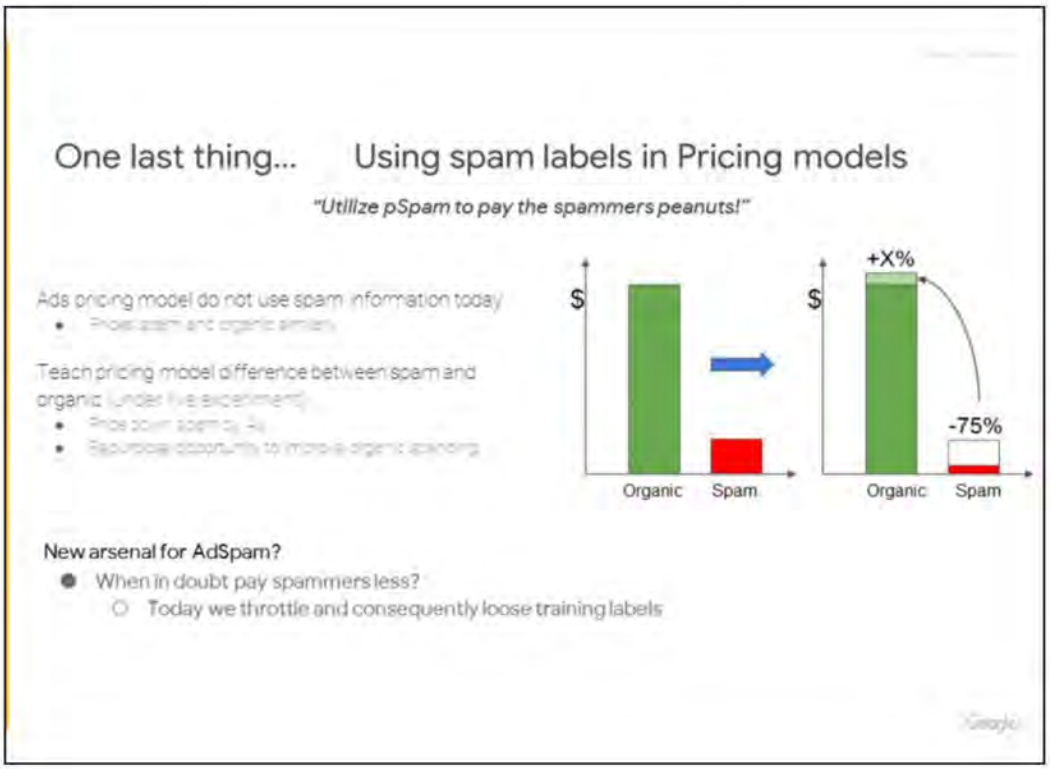


Monitoring Solution

Gaps	2020H1	2020H2
GoldStone monitoring limited to ASML	Demonstrate usefulness of GoldStone monitoring on Search and GDA filters	GoldStone to monitor all AdScam filtration
Handful of metrics used in quality monitoring	GoldStone integrated with ASTM. Currently uses 90 metrics	Add all possible metrics (~120). Integrate Bothets metrics
No SPRT, Manual blacklists monitoring		Deploy GoldStone and quantity monitoring for blacklist monitoring
Quantity monitoring spikes difficult to explain	Proof of concept with Graph Mining attributing slices to quantity spikes	Productionize and deploy alongside quantity monitoring
New launches require monitoring configuration changes	Demonstrate Ensemble Metric is adequate to monitor quality of all Search and GDA filters	Automatically monitor ***all*** models as soon as they hit live traffic

Google

Id	Date	Text
1	06/22/2020 18:34:23	+ykzhu@google.com please check if this aligns with our plans. _Assigned to Yong-Kang Zhu_

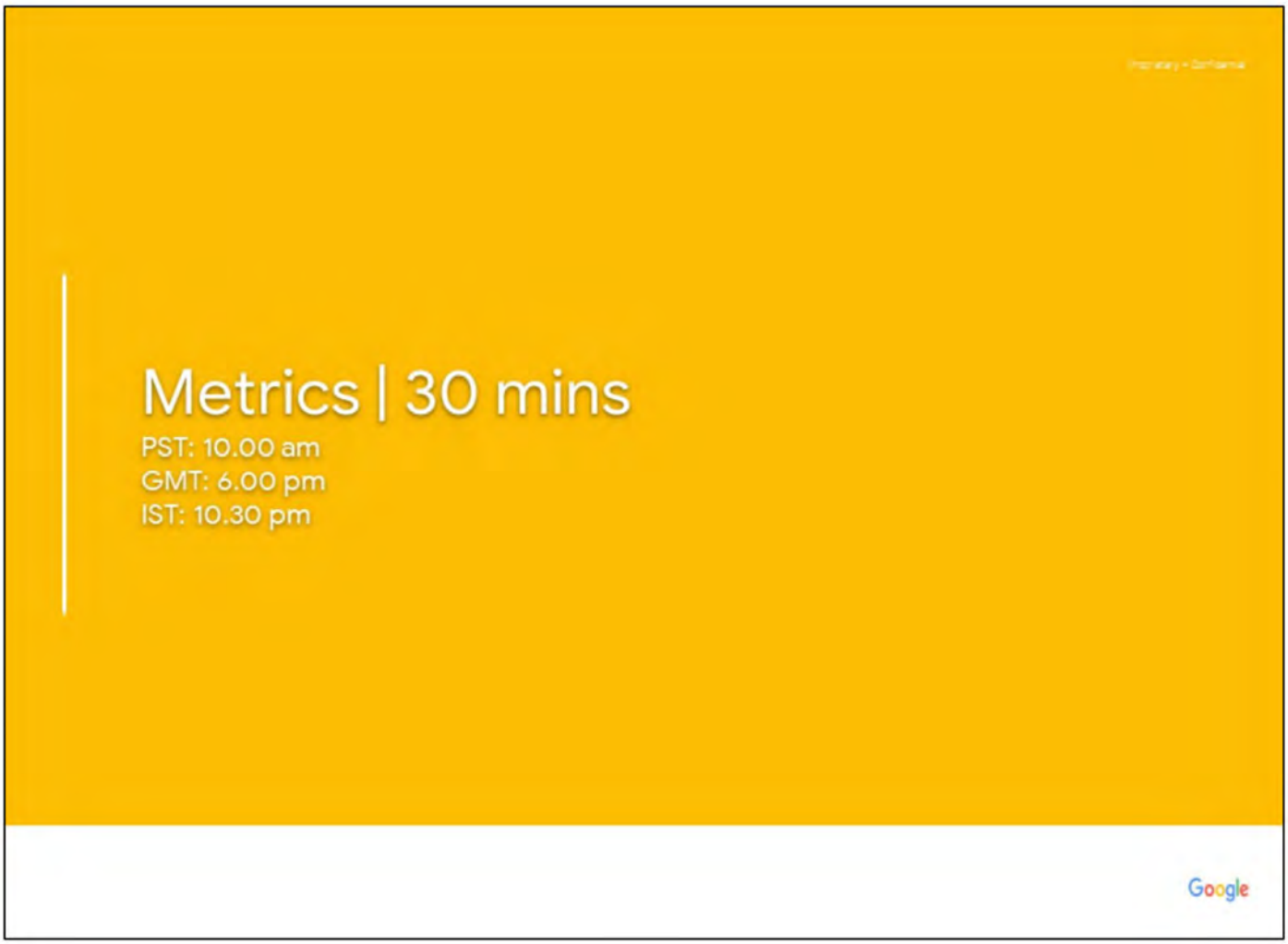

One last thing... Using spam labels in Pricing models
"Utilize pSpam to pay the spammers peanuts!"
Ads pricing model do not use spam information today
Teach pricing model difference between spam and organic
$
Organic
Spam
+X%
-75%
New arsenal for AdSpam?
When in doubt pay spammers less?
Today we throttle and consequently loose training labels

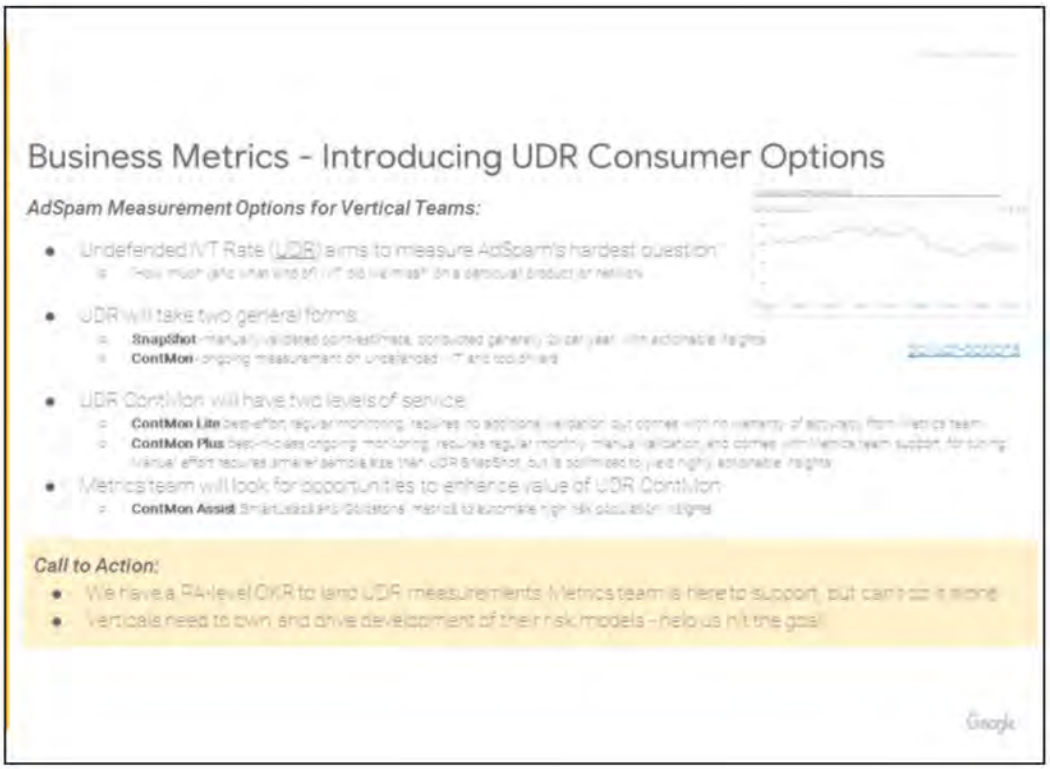
Break | 10 mins

PST: 9.50 am - 10.00 am
GMT: 5.50 pm - 6.00 pm
IST: 10.20 pm - 10.30 pm

Next session: Metrics

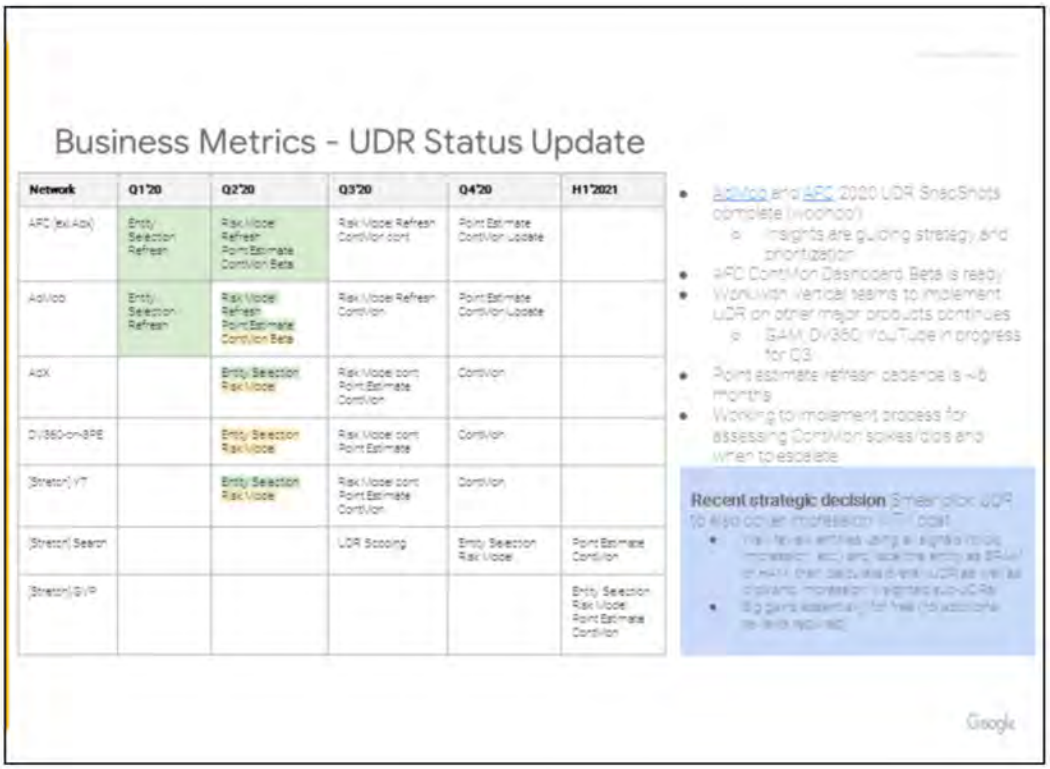
Google


Metrics | 30 mins
PST: 10.00 am
GMT: 6.00 pm
IST: 10.30 pm
Google



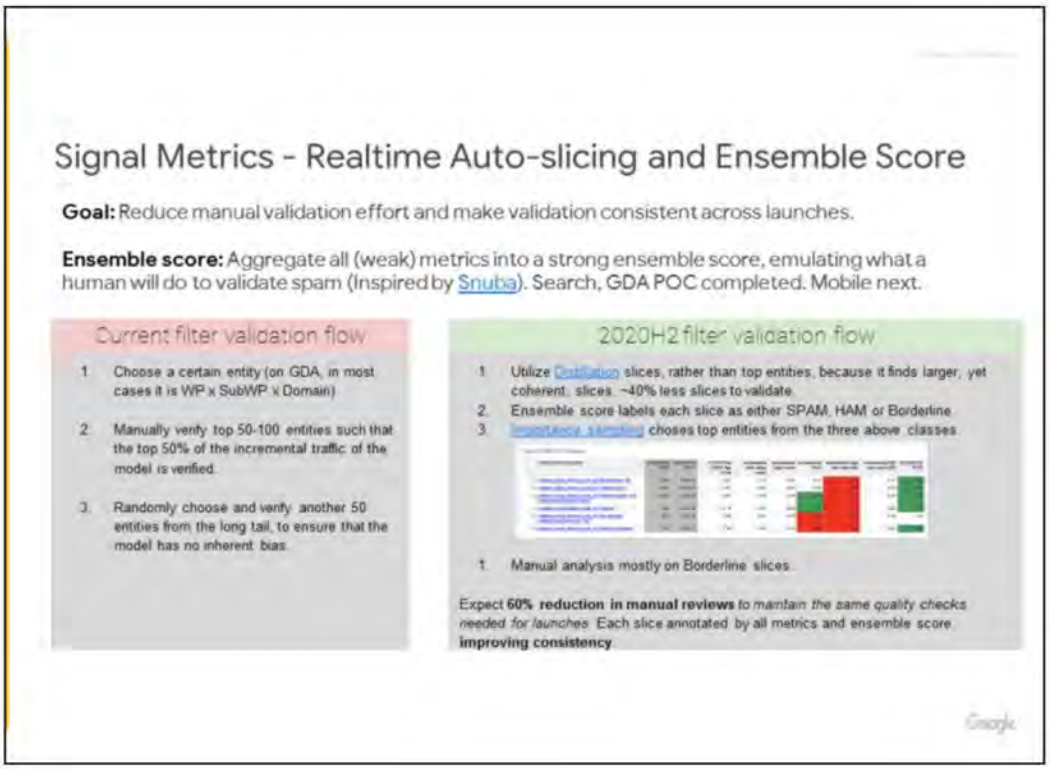
Speaker: Zack

Ads OKR: Land continuous monitoring dashboards for Undefended IVT Rate (UDR) for core ads product areas: AdSense, AdX, AdMob, DV360, and [STRETCH] Search, YouTube, and GVP.

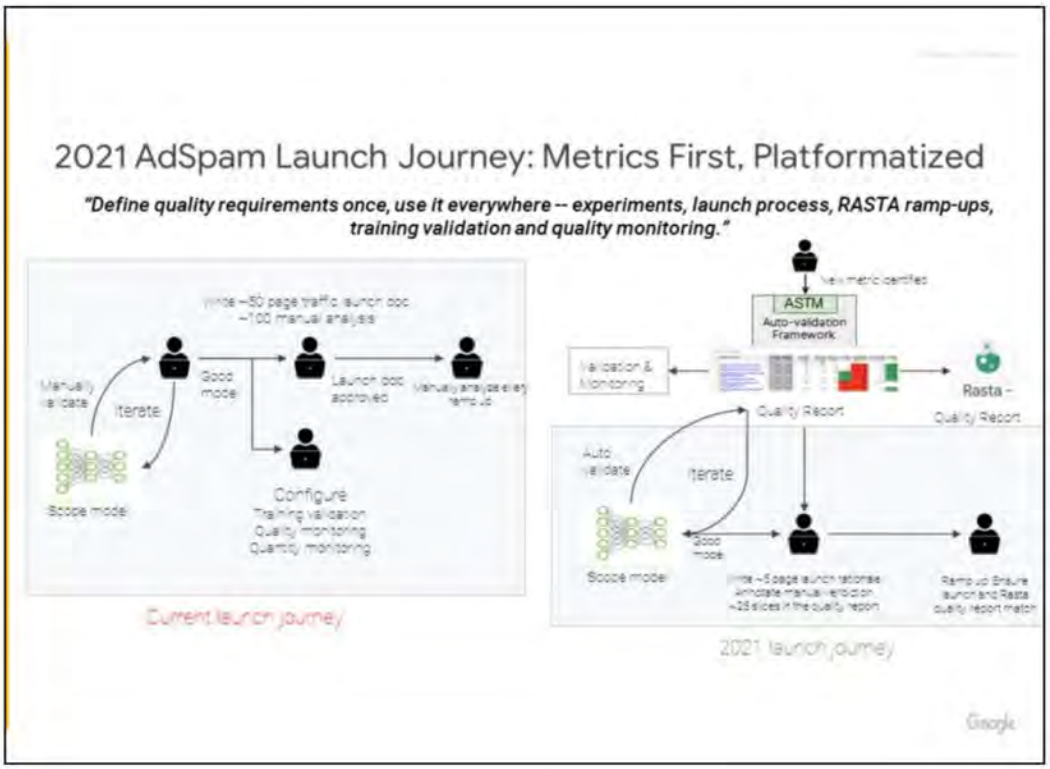


Speaker: Andrew

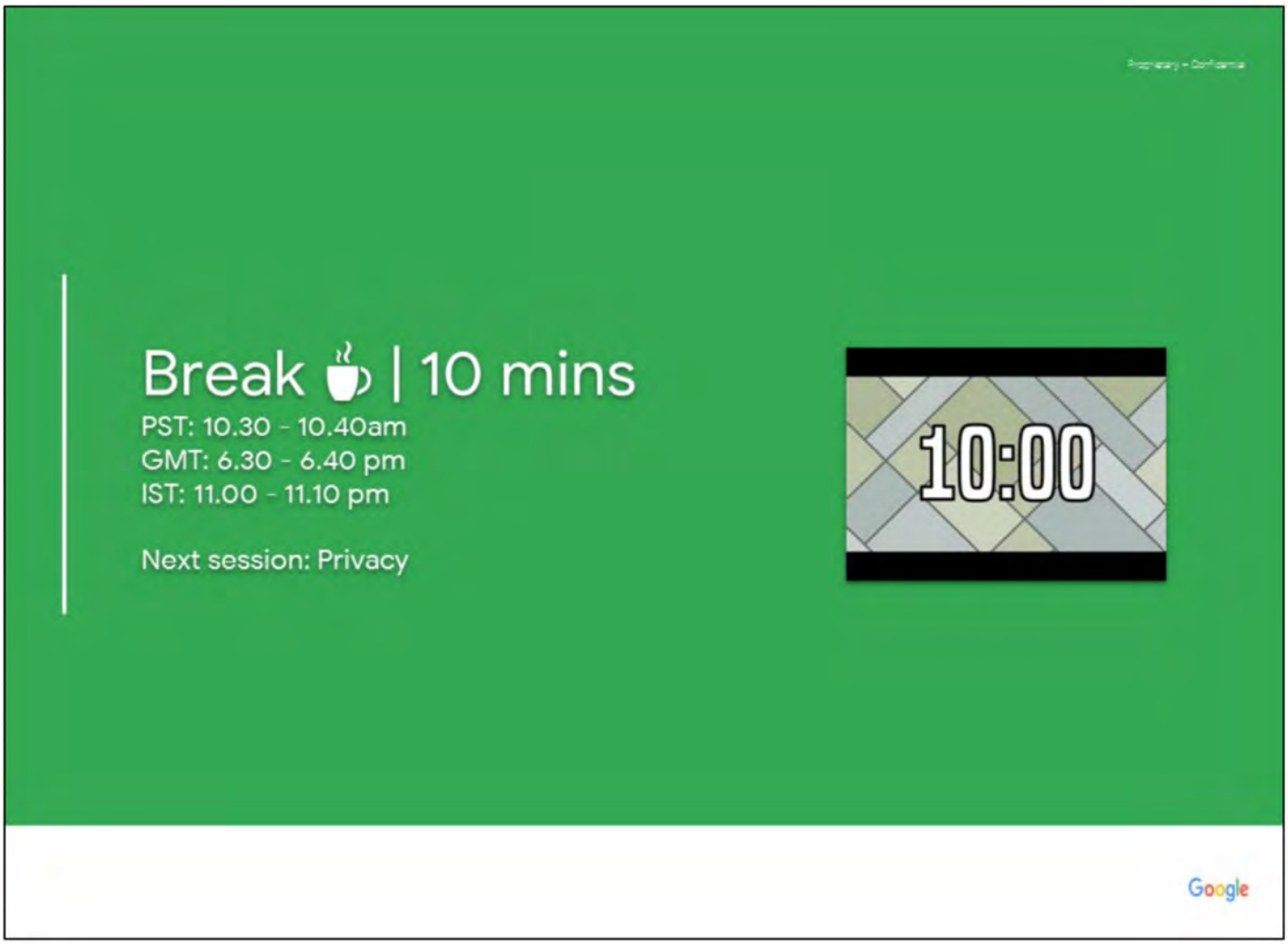
Speaker: Souvik

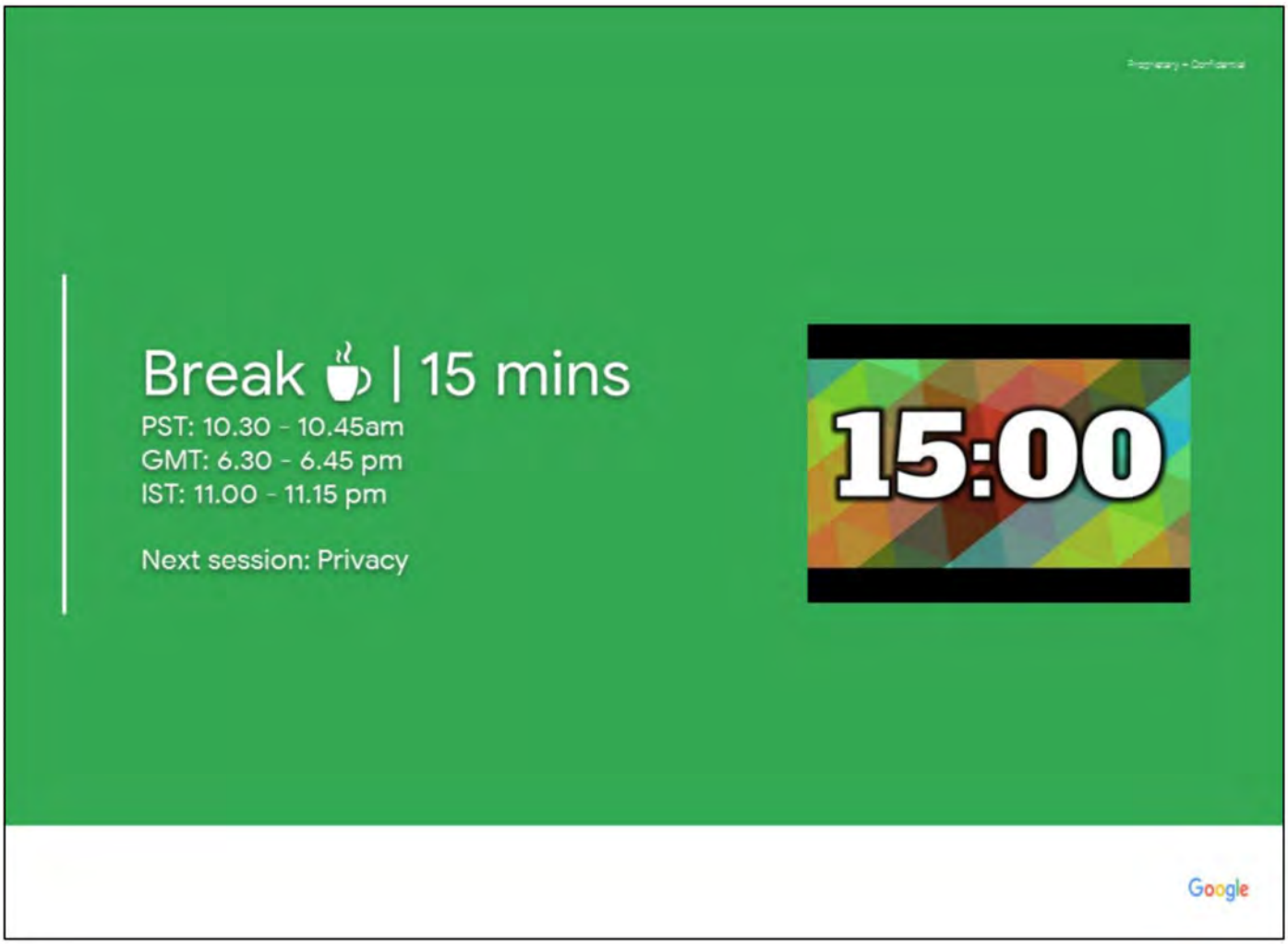


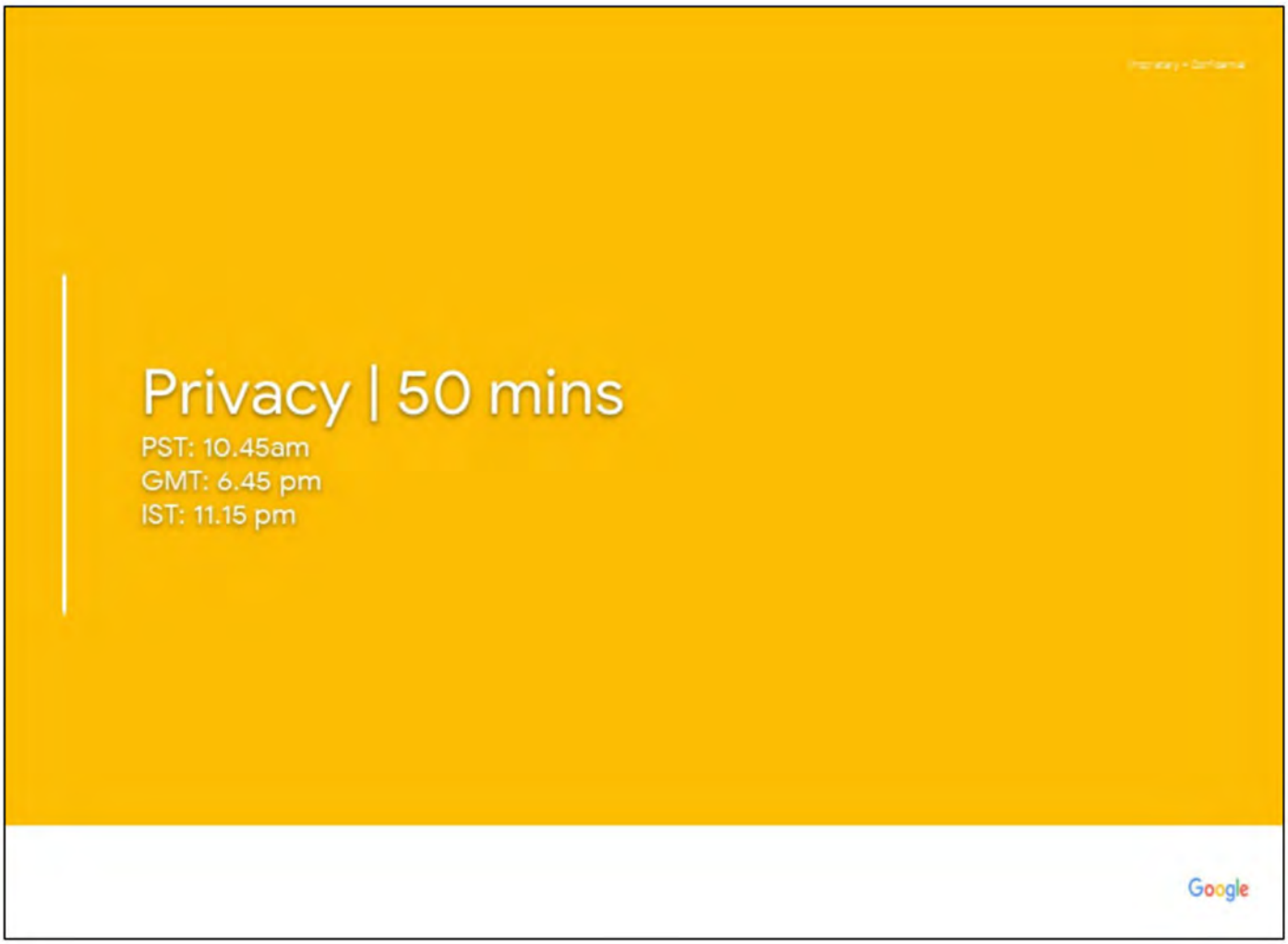
Speaker: Souvik

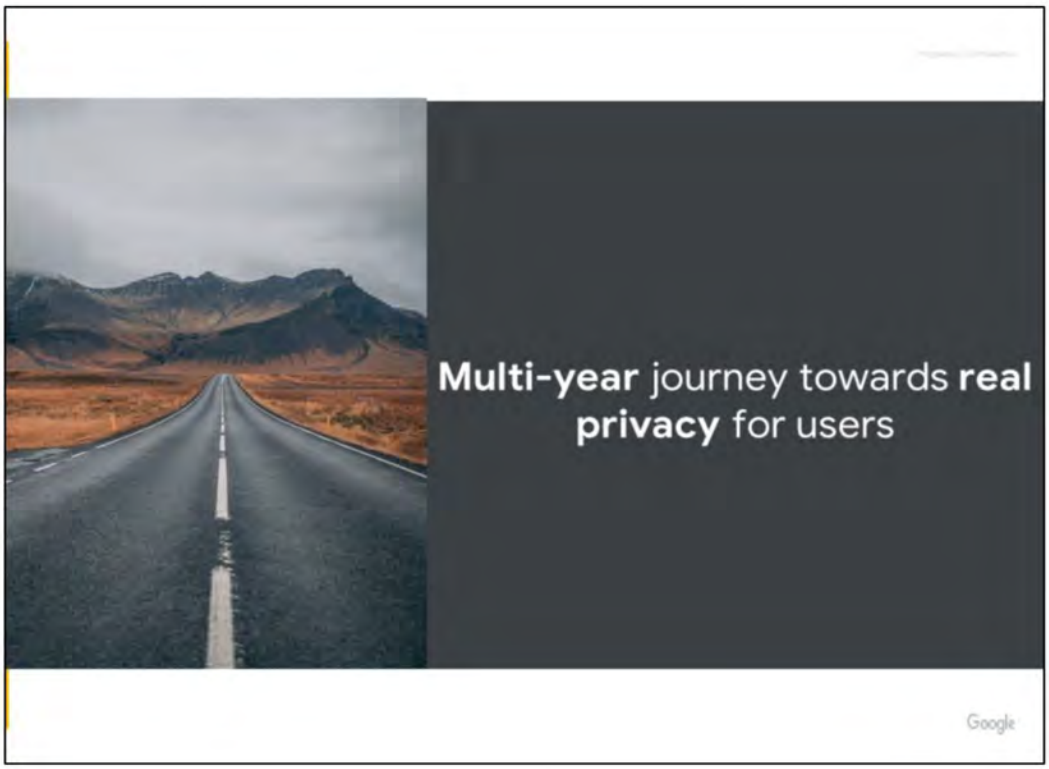


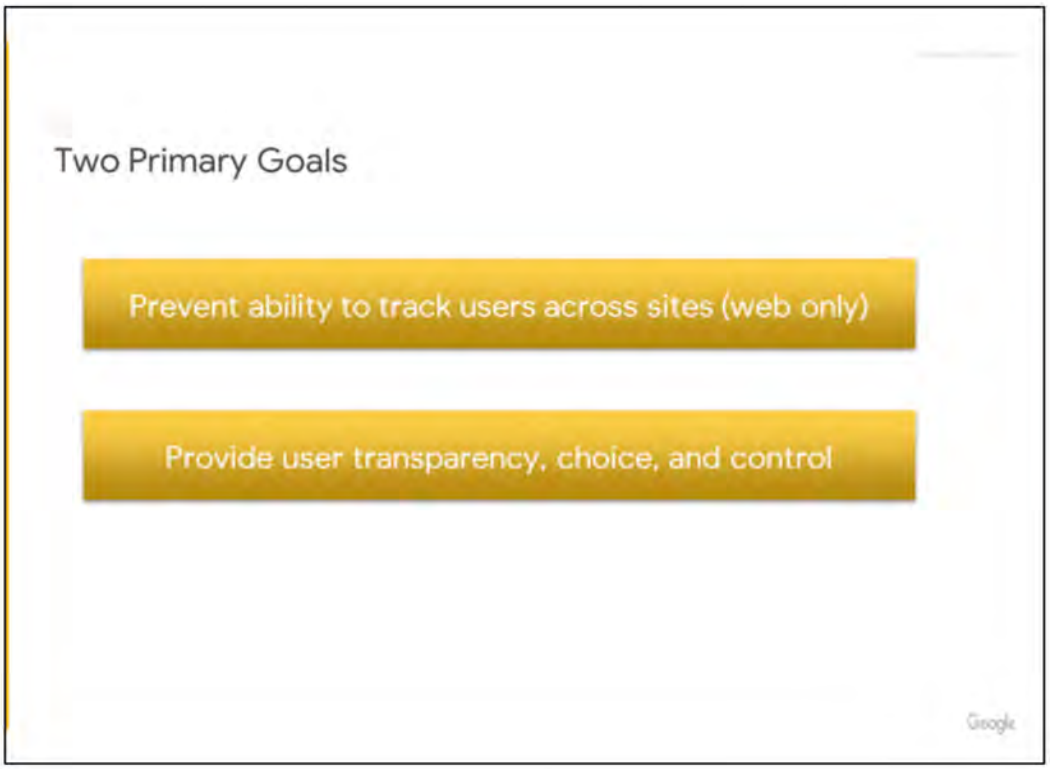
Speaker: Souvik

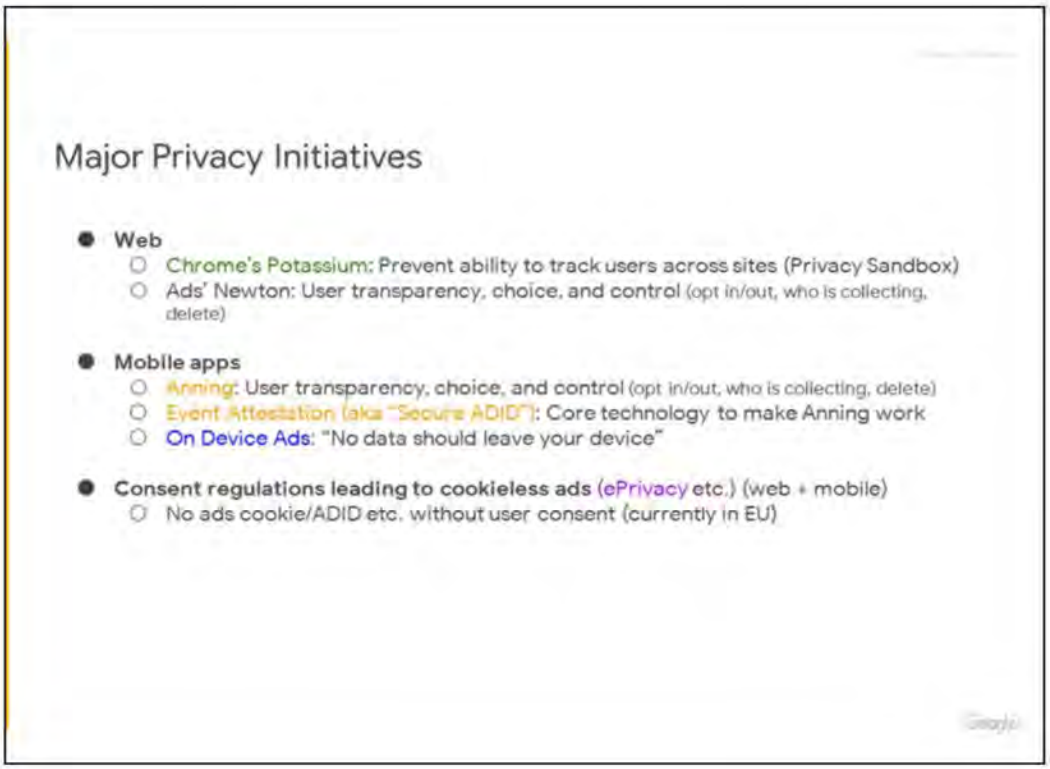

Break | 10 mins
PST: 10.30 - 10.40am
GMT: 6.30 - 6.40 pm
IST: 11.00 - 11.10 pm
Next session: Privacy
10:00
Google

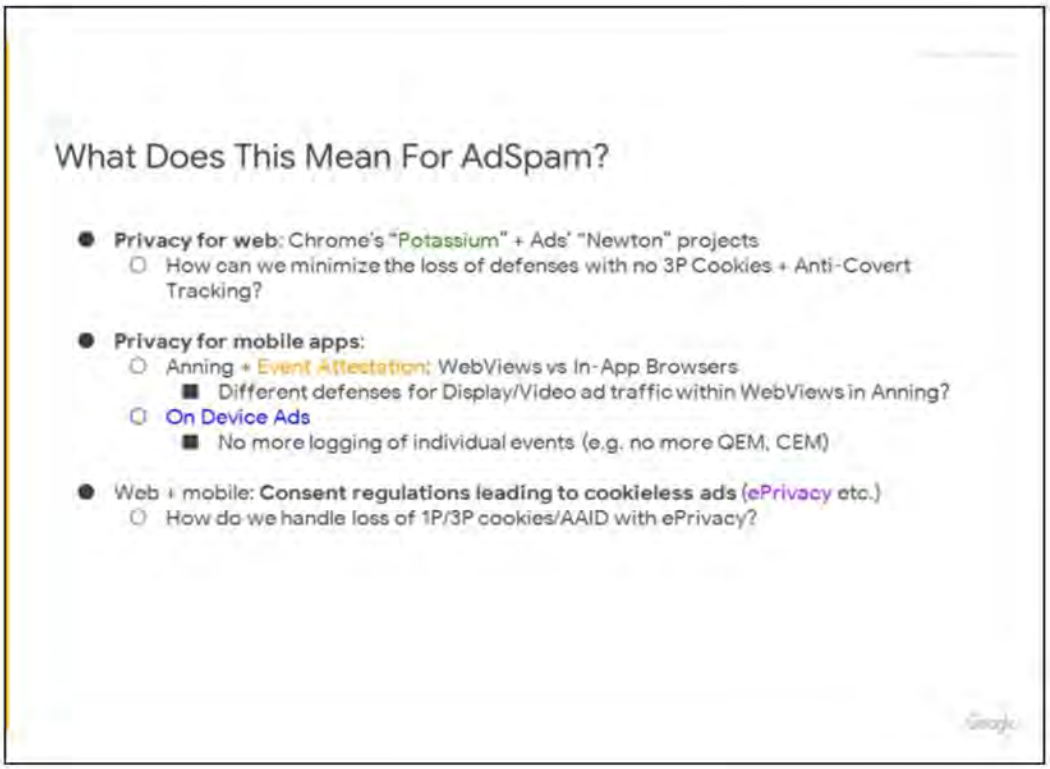

Break | 15 mins
PST: 10.30 - 10.45am
GMT: 6.30 - 6.45 pm
IST: 11.00 - 11.15 pm
Next session: Privacy
15:00
Google

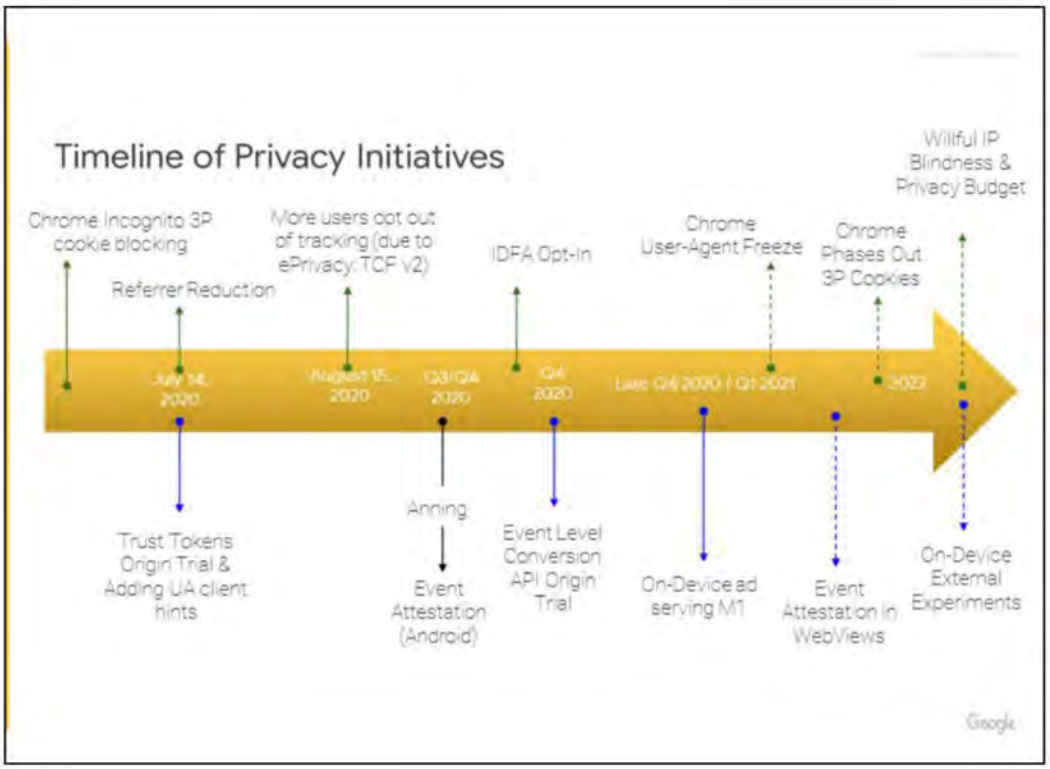

Privacy | 50 mins
PST: 10.45am
GMT: 6.45 pm
IST: 11.15 pm
Google

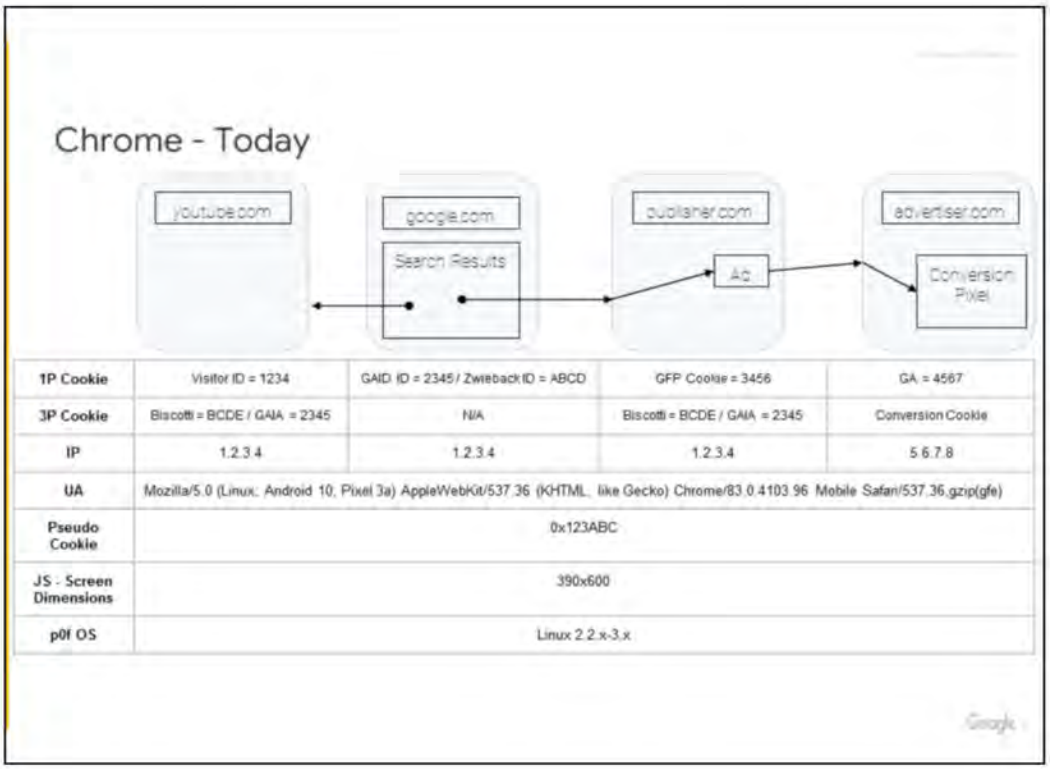

Multi-year journey towards real privacy for users
Google


Two Primary Goals
Prevent ability to track users across sites (web only)
Provide user transparency, choice, and control
Google

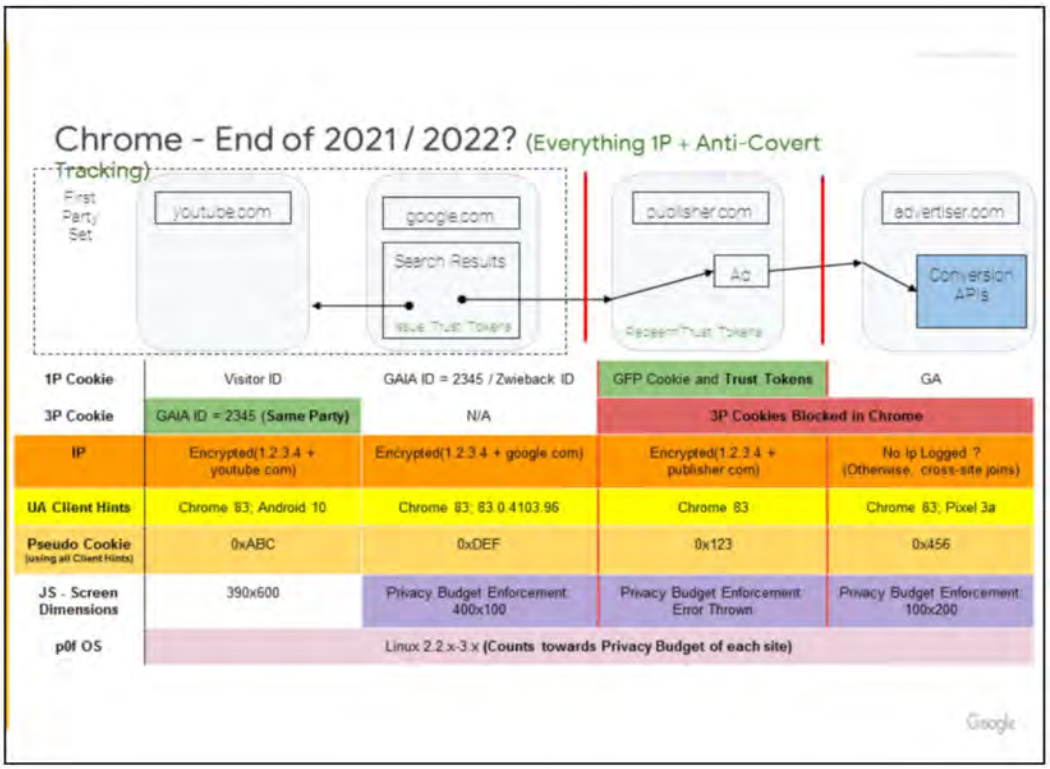

Major Privacy Initiatives
Web
Chrome's Potassium: Prevent ability to track users across sites (Privacy Sandbox)
Ads' Newton: User transparency, choice, and control (opt in/out, who is collecting, delete)
Mobile apps
Anning: User transparency, choice, and control (opt in/out, who is collecting, delete)
Event Attestation (aka "Secure ADID"): Core technology to make Anning work
On Device Ads: "No data should leave your device"
Consent regulations leading to cookieless ads (ePrivacy etc.) (web + mobile)
No ads cookie/ADID etc. without user consent (currently in EU)


What Does This Mean For AdSpam?
Privacy for web: Chrome's "Potassium" + Ads' "Newton" projects
How can we minimize the loss of defenses with no 3P Cookies + Anti-Covert Tracking?
Privacy for mobile apps:
Anning + Event Attestation: WebViews vs In-App Browsers
Different defenses for Display/Video ad traffic within WebViews in Anning?
On Device Ads
No more logging of individual events (e.g. no more QEM, CEM)
Web + mobile: Consent regulations leading to cookieless ads (ePrivacy etc.)
How do we handle loss of 1P/3P cookies/AAID with ePrivacy?


Timeline of Privacy Initiatives
Willful IP Blindness & Privacy Budget
Chrome Incognito 3P cookie blocking
More users opt out of tracking (due to ePrivacy, TCF v2)
IDFA Opt-In
Chrome User-Agent Freeze
Chrome Phases Out 3P Cookies
Referrer Reduction
July 14, 2020
August 15, 2020
Q3/Q4 2020
Q4 2020
Late Q4 2020 / Q1 2021
2022
Trust Tokens Origin Trial & Adding UA client hints
Anning
Event Attestation (Android)
Event Level Conversion API Origin Trial
On-Device ad serving M1
Event Attestation in WebViews
On-Device External Experiments
Google



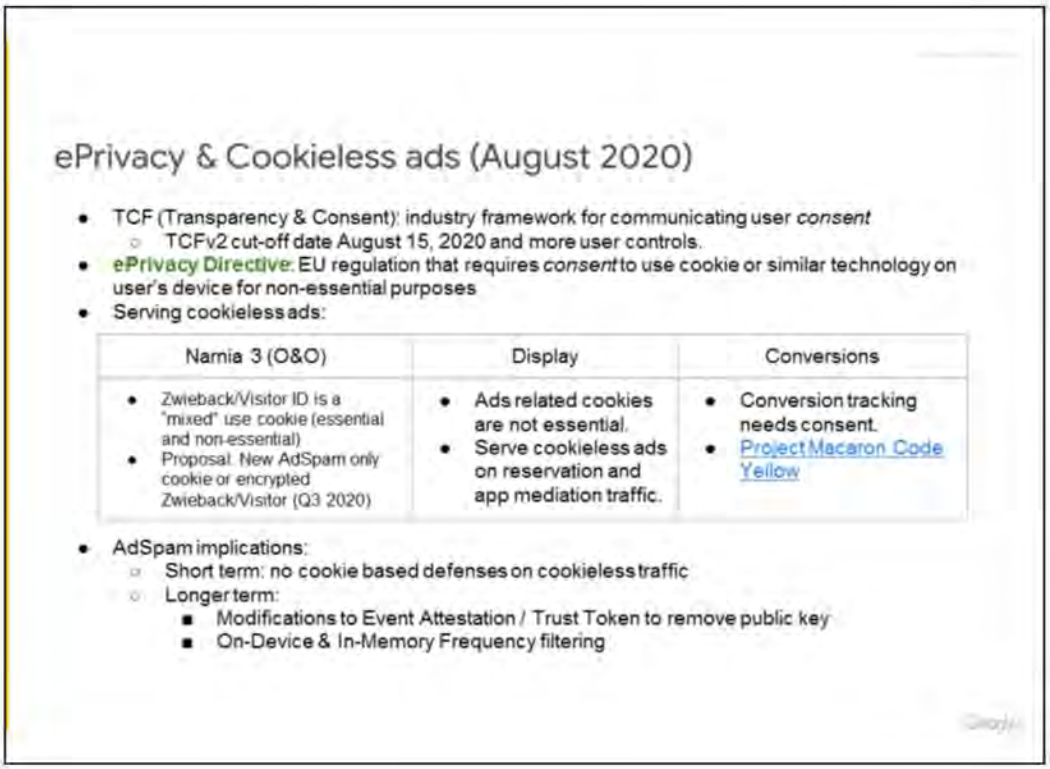
1P Cookie	Visitor ID = 1234	GAID ID = 2345 / Zwieback ID = ABCD	GFP Cookie = 3456	GA = 4567
3P Cookie	Biscotti = BCDE / GAIA = 2345	N/A	Biscotti = BCDE / GAIA = 2345	Conversion Cookie
IP	1.2.3.4	1.2.3.4	1.2.3.4	5.6.7.8
UA	Mozilla/5.0 (Linux; Android 10; Pixel 3a) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.96 Mobile Safari/537.36,gzip(gfe)			
Pseudo Cookie	0x123ABC			
JS - Screen Dimensions	390x600			
p0f OS	Linux 2.2.x-3.x			



KEY TAKEAWAY: Can't track users cross-site (only within same "company")

Research we need to explore?

- How can we achieve cross-site based filters (e.g. co-click) with help from Chrome?
  - Chrome's proposed Aggregated Reporting API
  - FLoC IDs?
  - Bloom filters in Chrome with Differential Privacy?
  - Crypto (Secure Multi-party Computation) + Cloud ML?
- Anti-abuse teams want IPs, but Chrome wants us to move away from IPs
  - We're always asked if we can rely less on fingerprinting and more on Trust Tokens
- Can we build defenses only on 1P information with privacy budget enforcement?
- How well will CG (Q3) and Conversion Spam work with Differential Privacy?
- Optimal 1P Trust Token Issuance logic and developing 3rd party issuers (e.g. whiteops tokens)
- How much entropy does AdSpam need w.r.t a privacy budget?
- Effectiveness of Albus and third party IVT detection within Chrome Privacy Sandbox?

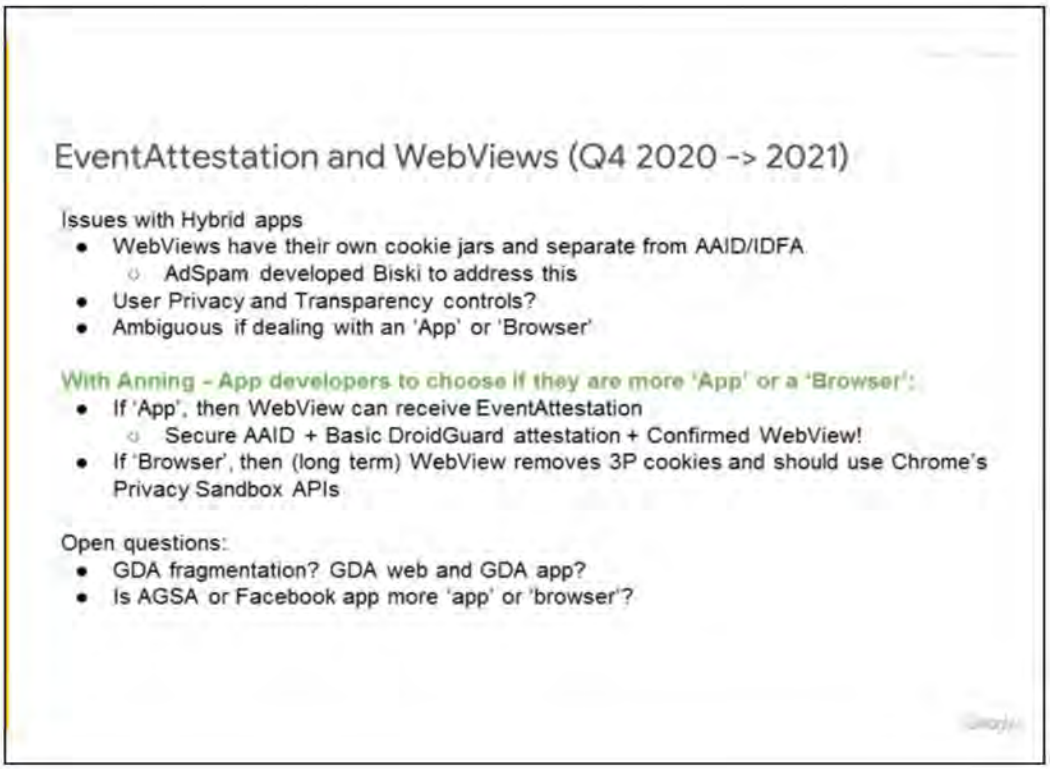


ePrivacy & Cookieless ads (August 2020)

- TCF (Transparency & Consent): industry framework for communicating user *consent*
  - TCFv2 cut-off date August 15, 2020 and more user controls.
- **ePrivacy Directive**: EU regulation that requires *consent* to use cookie or similar technology on user's device for non-essential purposes
- Serving cookieless ads:

Narnia 3 (O&O)	Display	Conversions
• Zwieback/Visitor ID is a "mixed" use cookie (essential and non-essential) • Proposal: New AdSpam only cookie or encrypted Zwieback/Visitor (Q3 2020)	• Ads related cookies are not essential. • Serve cookieless ads on reservation and app mediation traffic.	• Conversion tracking needs consent. • Project Macaron Code Yellow

- AdSpam implications:
  - Short term: no cookie based defenses on cookieless traffic
  - Longer term:
    - Modifications to Event Attestation / Trust Token to remove public key
    - On-Device & In-Memory Frequency filtering



EventAttestation and WebViews (Q4 2020 -> 2021)

Issues with Hybrid apps

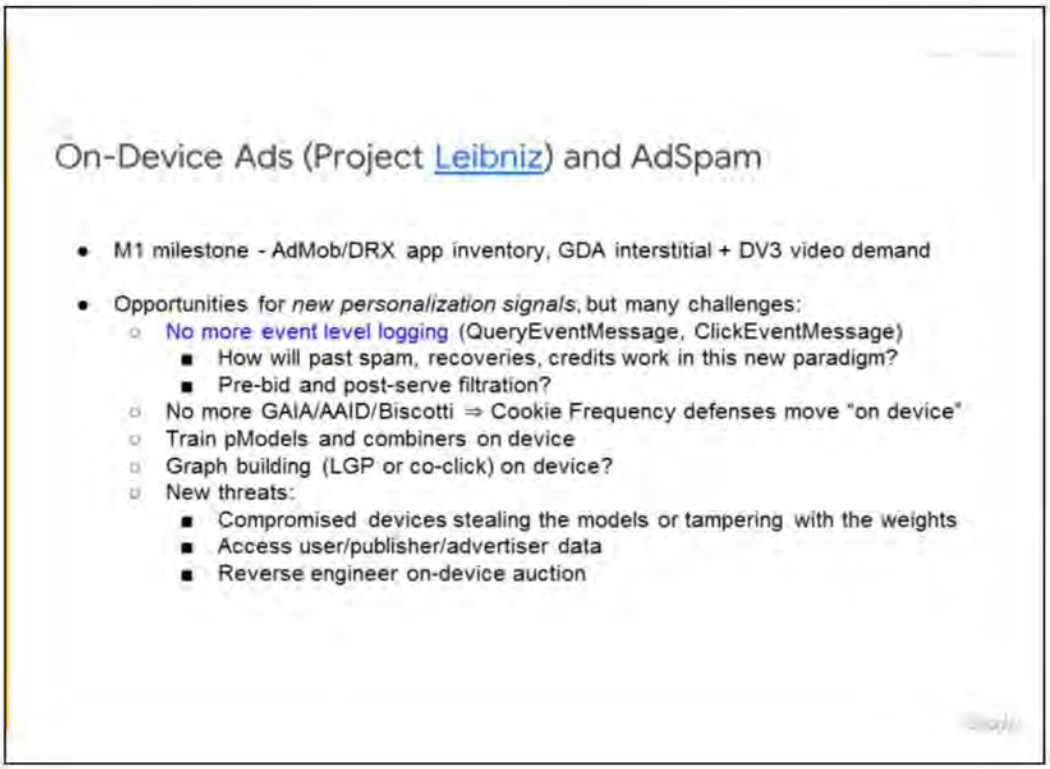
- WebViews have their own cookie jars and separate from AAID/IDFA
  - AdSpam developed Biski to address this
- User Privacy and Transparency controls?
- Ambiguous if dealing with an 'App' or 'Browser'

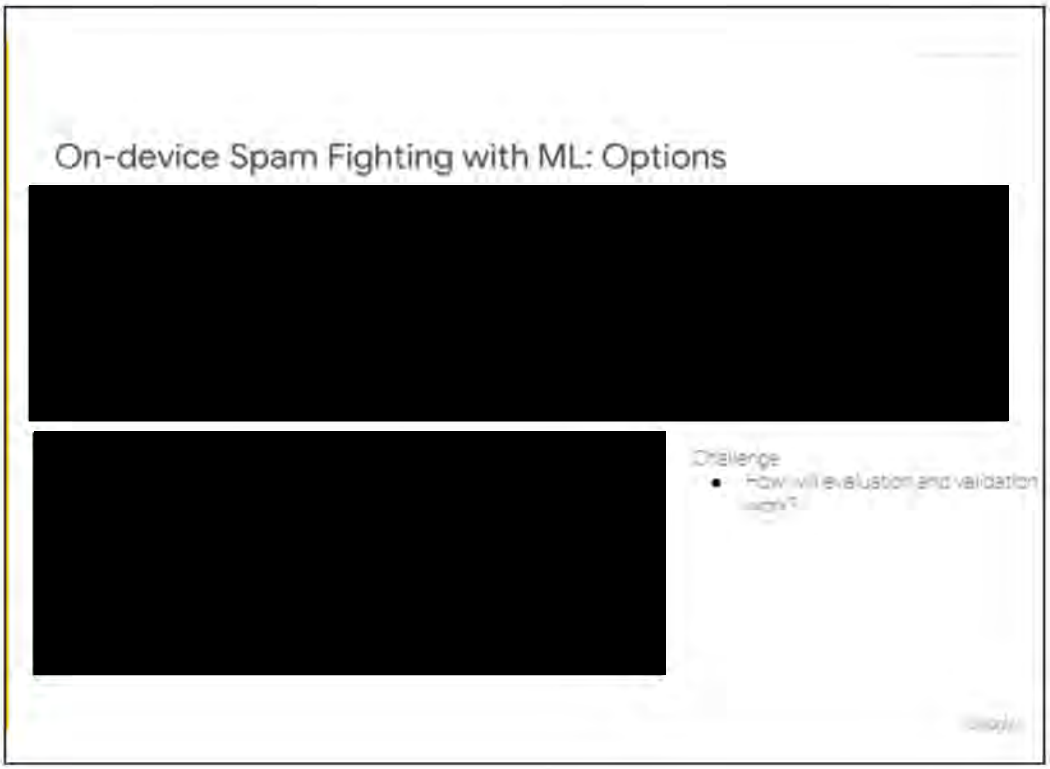
With Anning - App developers to choose if they are more 'App' or a 'Browser':

- If 'App', then WebView can receive EventAttestation
  - Secure AAID + Basic DroidGuard attestation + Confirmed WebView!
- If 'Browser', then (long term) WebView removes 3P cookies and should use Chrome's Privacy Sandbox APIs

Open questions:

- GDA fragmentation? GDA web and GDA app?
- Is AGSA or Facebook app more 'app' or 'browser'?


On-Device Ads (Project Leibniz) and AdSpam
M1 milestone - AdMob/DRX app inventory, GDA interstitial + DV3 video demand
Opportunities for new personalization signals, but many challenges:
No more event level logging (QueryEventMessage, ClickEventMessage)
How will past spam, recoveries, credits work in this new paradigm?
Pre-bid and post-serve filtration?
No more GAIA/AAID/Biscotti ⇒ Cookie Frequency defenses move "on device"
Train pModels and combiners on device
Graph building (LGP or co-click) on device?
New threats:
Compromised devices stealing the models or tampering with the weights
Access user/publisher/advertiser data
Reverse engineer on-device auction

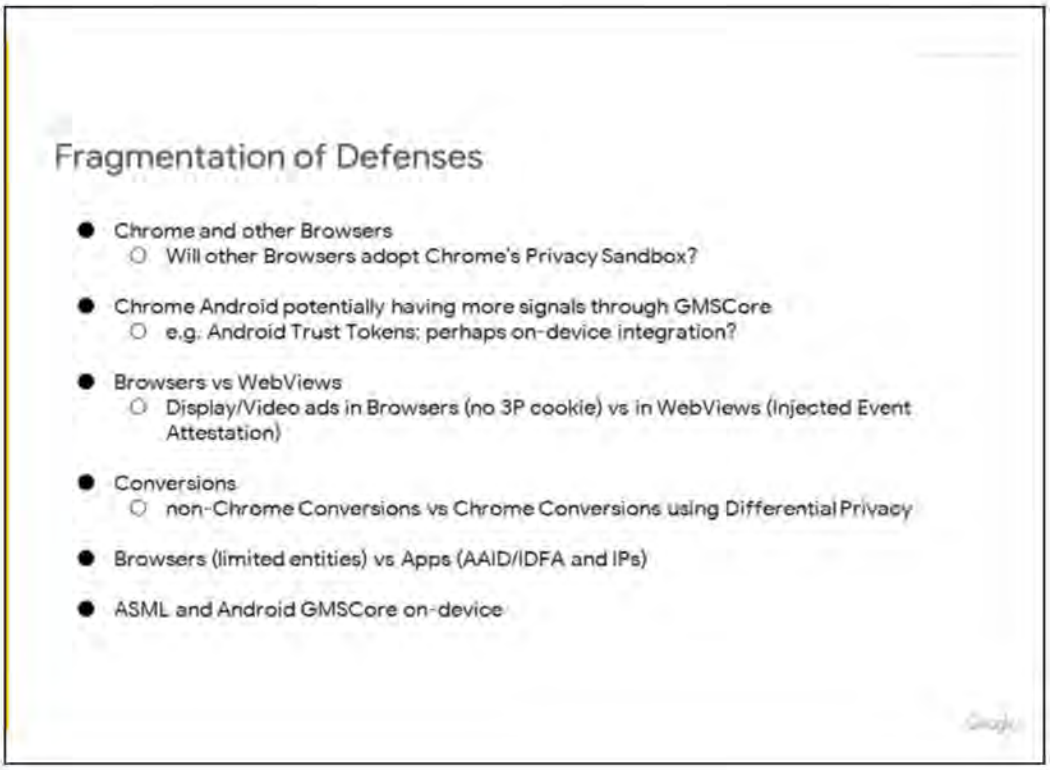

On-device Spam Fighting with ML: Options
[redacted]
[redacted]
Challenge
• How will evaluation and validation work?

On-device Spam Fighting with ML: Options

"What if we have access to no events server-side, only aggregates?"

[redacted]

- Per-event prediction and enforcement on-device
- **Several challenges**
  - AdSpam Specific
    - How to build meaningful base model using only aggregated features?
    - How will model monitoring work under differential privacy?
    - Several techniques to "fine-tune". Which technique? How to validate without access to data?
  - General
    - How to prevent stealing and reverse engineering of model and enforcement mechanisms
    - Unclear serving feasibility at AdSpam scale
    - On-device model size, complexity constrained by memory and battery budget



Necessary "remedies", but leads to more complexity?

Call To Action

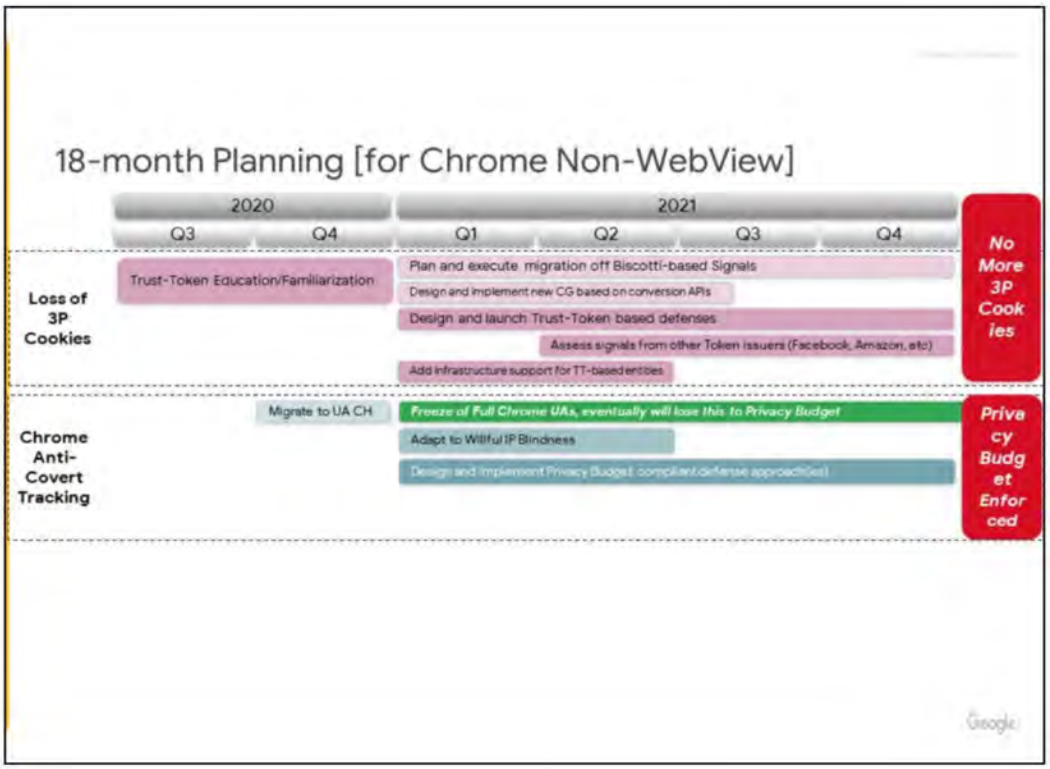
Privacy changes affecting AdSpam are starting **now**!

Be mindful of privacy changes that's coming within ~2 years vs longer term efforts (e.g. on device).

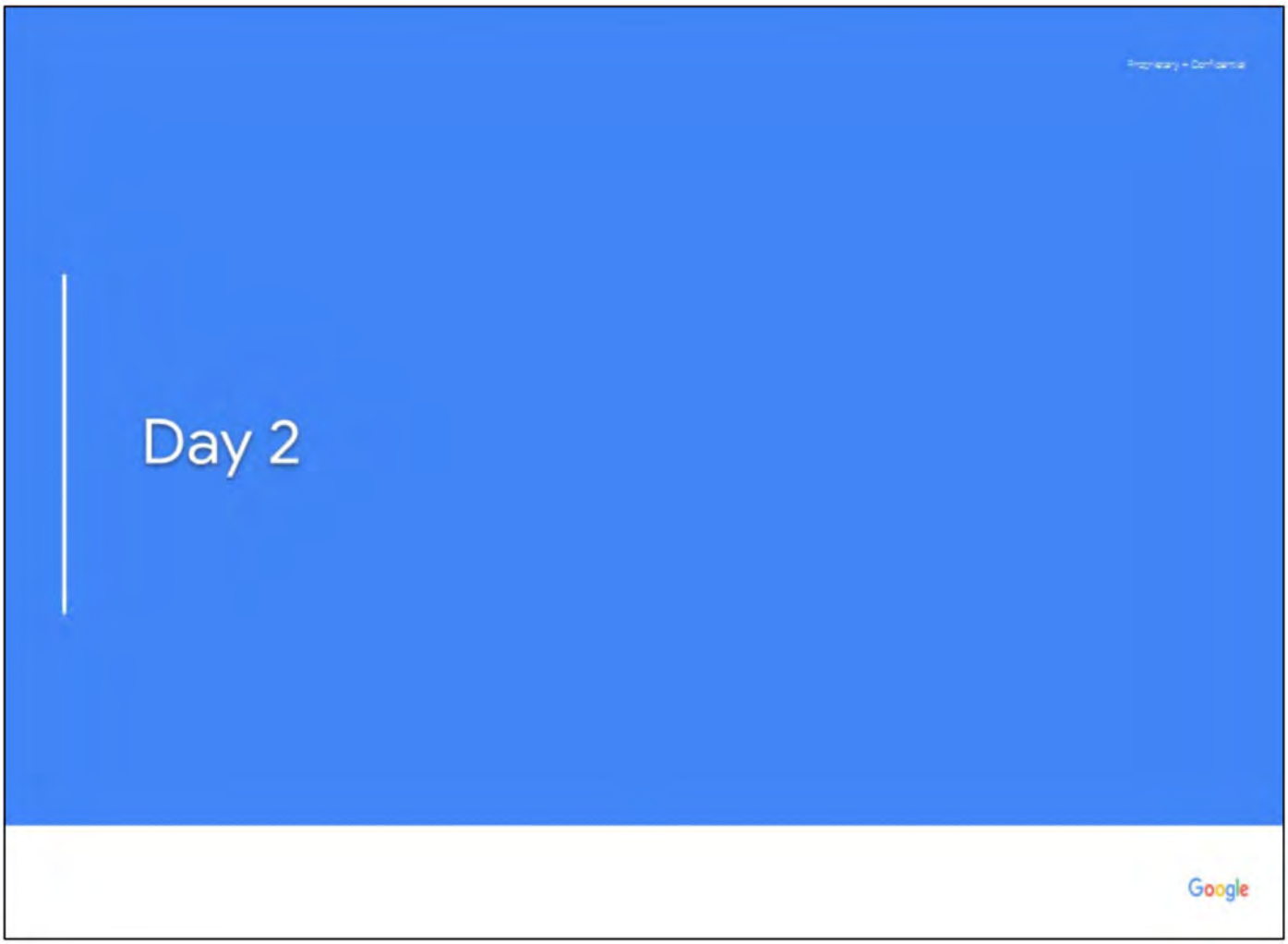
Do we continue to launch web-based defenses using entities/signals that we know are going away within 2 years (e.g., 3rd party cookies, detailed UA and IP, other high-entropy signals)?

Request teams start investing time in new web-based defenses using alternative signals and approaches.

Note: Privacy Team has limited resources with ~3 SWEs and 1 T&S


18-month Planning [for Chrome Non-WebView]
2020
2021
Q3
Q4
Q1
Q2
Q3
Q4
Loss of 3P Cookies
Trust-Token Education/Familiarization
Plan and execute migration off Biscotti-based Signals
Design and implement new CG based on conversion APIs
Design and launch Trust-Token based defenses
Assess signals from other Token issuers (Facebook, Amazon, etc)
Add infrastructure support for TT-based entities
No More 3P Cookies
Chrome Anti-Covert Tracking
Migrate to UA CH
Freeze of Full Chrome UAs, eventually will lose this to Privacy Budget
Adapt to Willful IP Blindness
Design and implement Privacy Budget compliant defense approach(es)
Privacy Budget Enforced
Google


Reminder
We (as Google) cannot violate the intentions of these privacy initiatives
(even if technically possible)


Day 2
Google

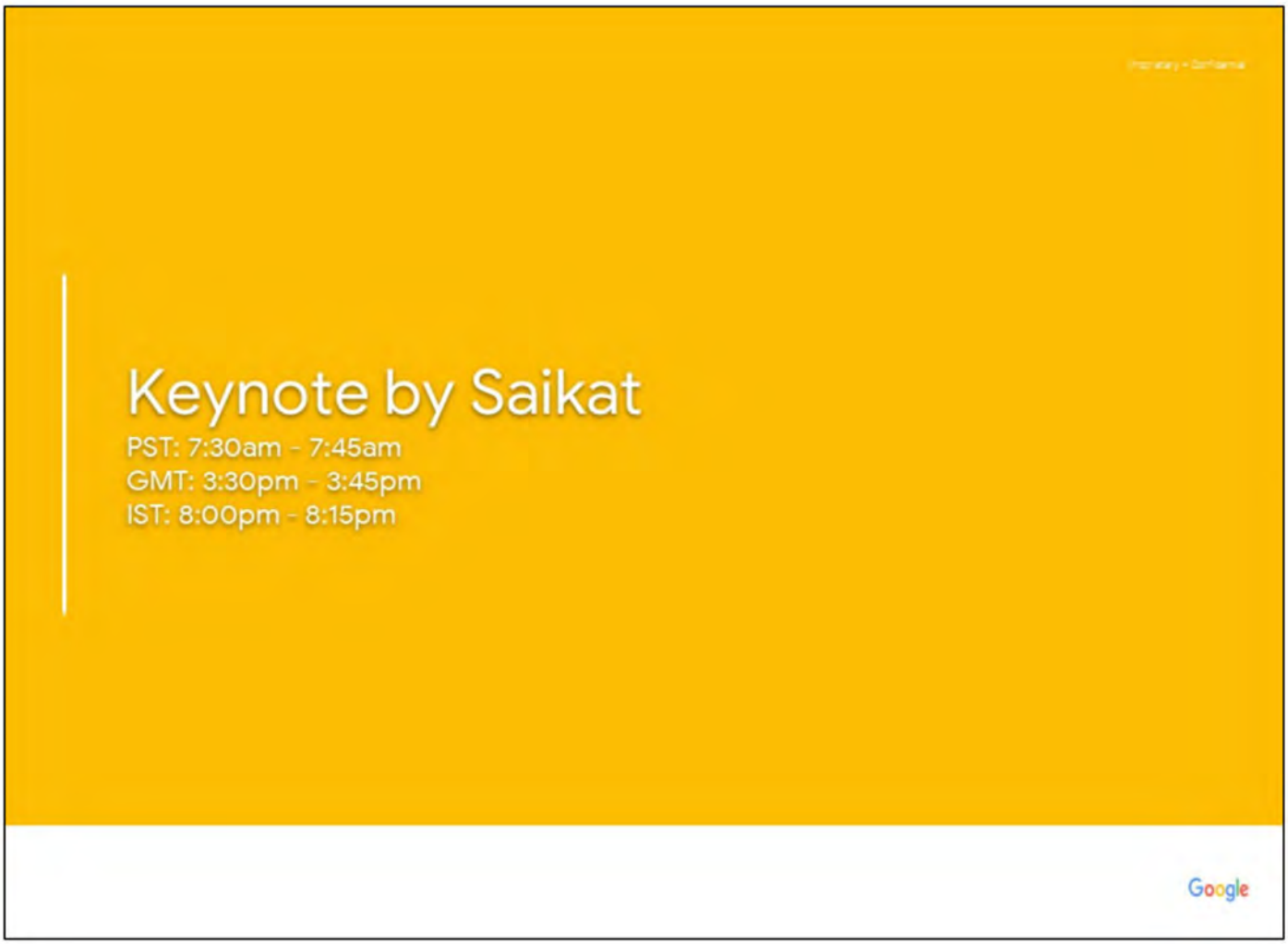
Agenda

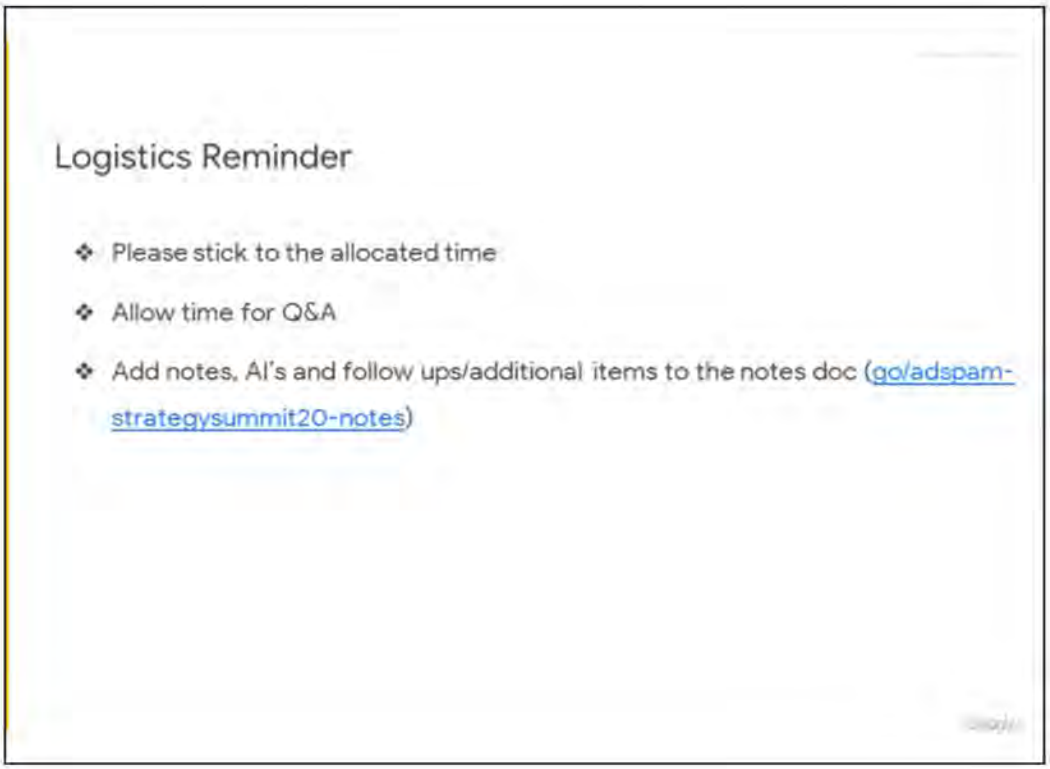
Day 2: Deep dives into key challenges

Keynote by Salkat
High level strategy overview
break
Trust Graph powered analysis
break
Challenges with supporting new/emerging markets/ segments/ products
Improving precision and monitoring
break
Impression Spam
Apps & Play
Closing Remarks
Fun event

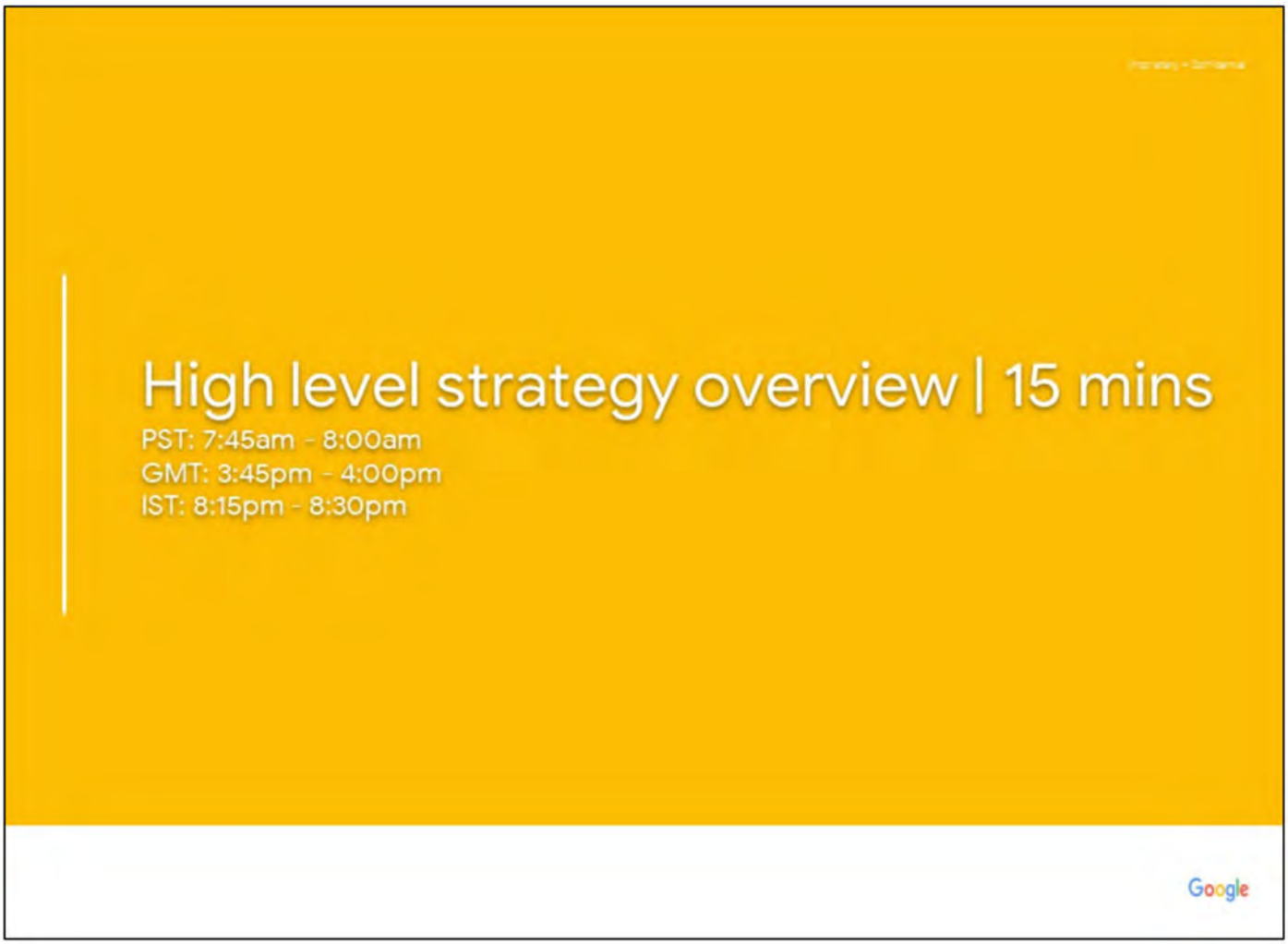
See detailed agenda at go/adscam-strategysummit20-agenda

Google

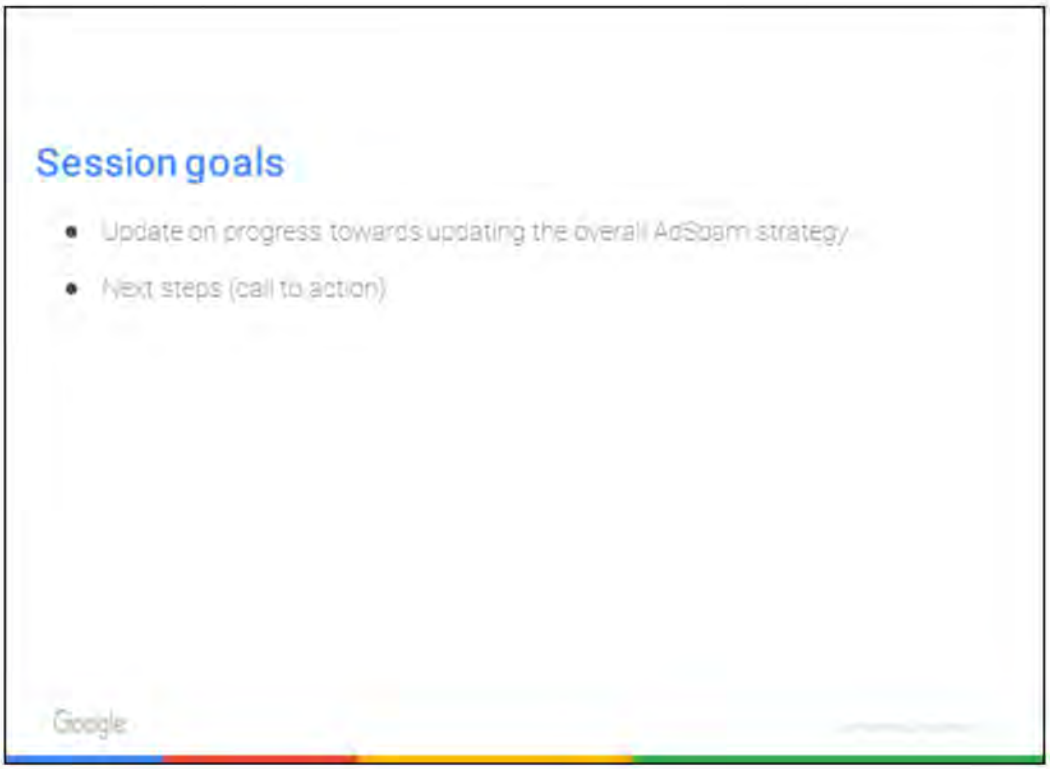

Keynote by Saikat
PST: 7:30am - 7:45am
GMT: 3:30pm - 3:45pm
IST: 8:00pm - 8:15pm
Google


Logistics Reminder
Please stick to the allocated time
Allow time for Q&A
Add notes, AI's and follow ups/additional items to the notes doc (go/adspam-strategysummit20-notes)

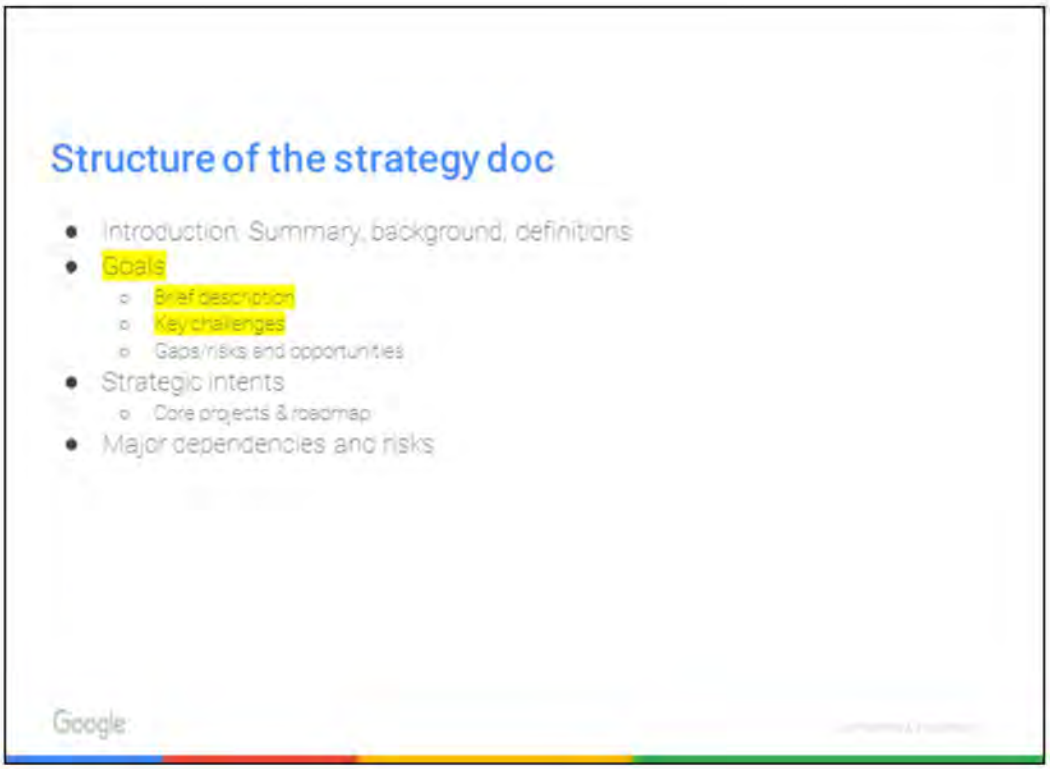
Misha - 40 sec

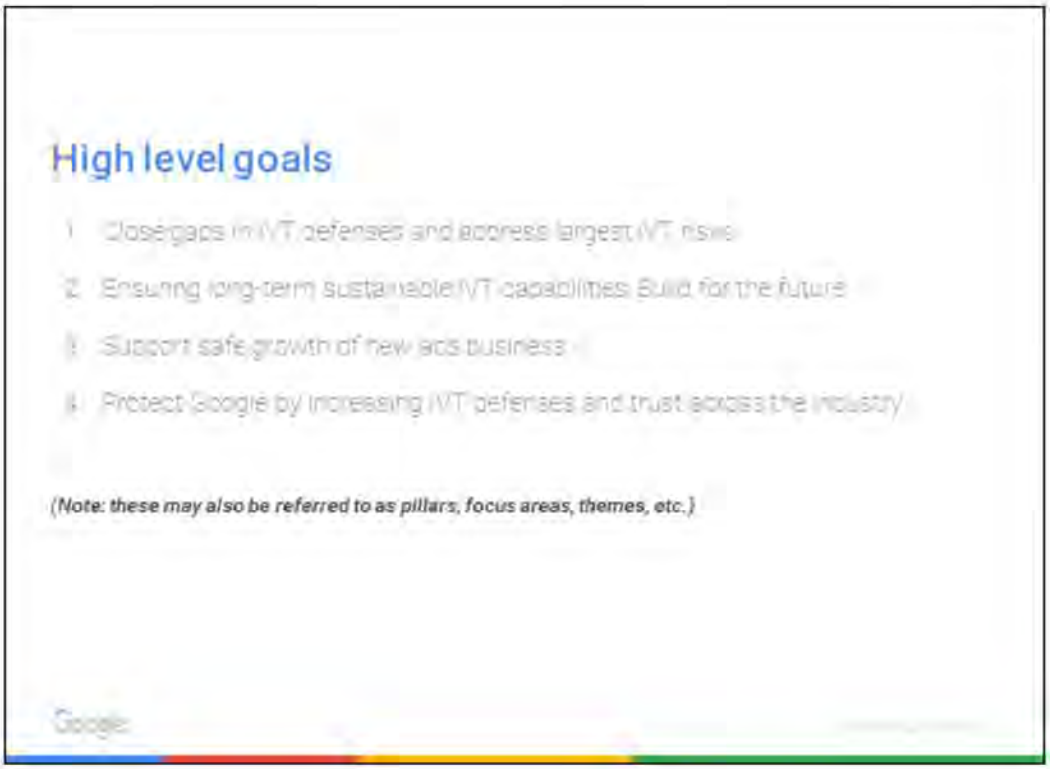

High level strategy overview | 15 mins
PST: 7:45am - 8:00am
GMT: 3:45pm - 4:00pm
IST: 8:15pm - 8:30pm
Google

Id	Date	Text
1	06/24/2020 04:49:32	+andresf@google.com +subir@google.com +aruna@google.com Added the strategy slides -- will check early Wed morning if you have suggestions for improvements.


Session goals
Update on progress towards updating the overall AdSpam strategy
Next steps (call to action)
Google

New platform/infra allows us to take it to the next level - what innovations can we build on top of our infra?
We are developing new and promising approaches - clustering, risk modeling, organic labeling, etc.
We are getting much better at leveraging data across Google
Industry collaboration, standards, and hardening the ecosystem is gaining momentum
I think we are ready for take-off to new levels of IVT defenses.


Structure of the strategy doc
Introduction. Summary, background, definitions
Goals
Brief description
Key challenges
Gaps/risks and opportunities
Strategic intents
Core projects & roadmap
Major dependencies and risks
Google



1) Close gaps in IVT defenses and address largest IVT risks
Minimize IVT risk by addressing areas with weak defenses across Google's ads products, and address the largest IVT risks.
2) Ensuring long-term sustainable IVT capabilities: Build for the future
Ensure that AdSpam is able to effectively protect Google's ads business in the future: win the arms race with bad actors, adapt to ongoing shifts in privacy approaches and other ecosystem changes, and evolve in tandem with Google's ads products.
3) Support safe growth of new ads business
Support the sustainable growth of new business opportunities like new ad products, new formats, new environments, new deals, etc. across all of Google's ad product portfolio.
4) Protect Google by increasing IVT defenses and trust across the industry
In order to effectively fight and prevent IVT and ad fraud within Google, we need to increase IVT defenses and trust across the industry at large to minimize overall systemic risk.

1) Close gaps in IVT defenses and address largest IVT risks

Description: Minimize IVT risk by addressing areas with weak defenses across Google's ads products, and address the largest IVT risks.

Challenges:

- Large number of surfaces to defend (products, formats, devices, event types, logs, etc.)
- Adversarial nature means we can't launch in a "set it and forget it" mode
- Sophisticated fraud is attractive for some companies and cyber criminals
  - They are highly skilled and can mount sophisticated and scalable IVT operations (attacks)

Google

2) Ensure long-term sustainable IVT capabilities: Build for the future

Description: Ensure that AdSpam is able to effectively protect Google's ads business in the future: win the arms race with bad actors, adapt to ongoing shifts in privacy approaches and other ecosystem changes, and evolve in tandem with Google's ads products.

Challenges: Developing a deeper understanding, more comprehensive knowledge, and better methods, tools, and techniques to

- scale with Google's evolving ads products
- adapt to dynamic and increasingly sophisticated bad actors
- maintain defenses in the new privacy-first online environment.

Google

3) Support safe growth of new ads business

Description: Support the sustainable growth of new business opportunities like new ad products, new formats, new environments, new deals, etc. across all of Google's ad product portfolio.

Challenges:

- Providing IVT defenses for new products and deals that may not "fit the mold"
  - new interaction models
  - not using "standard" ads backends (e.g., logs)
- Supporting custom deals while maintaining economy of scale and avoiding one-off solutions
- Achieving defensibility in environments that lack signal collection

Google

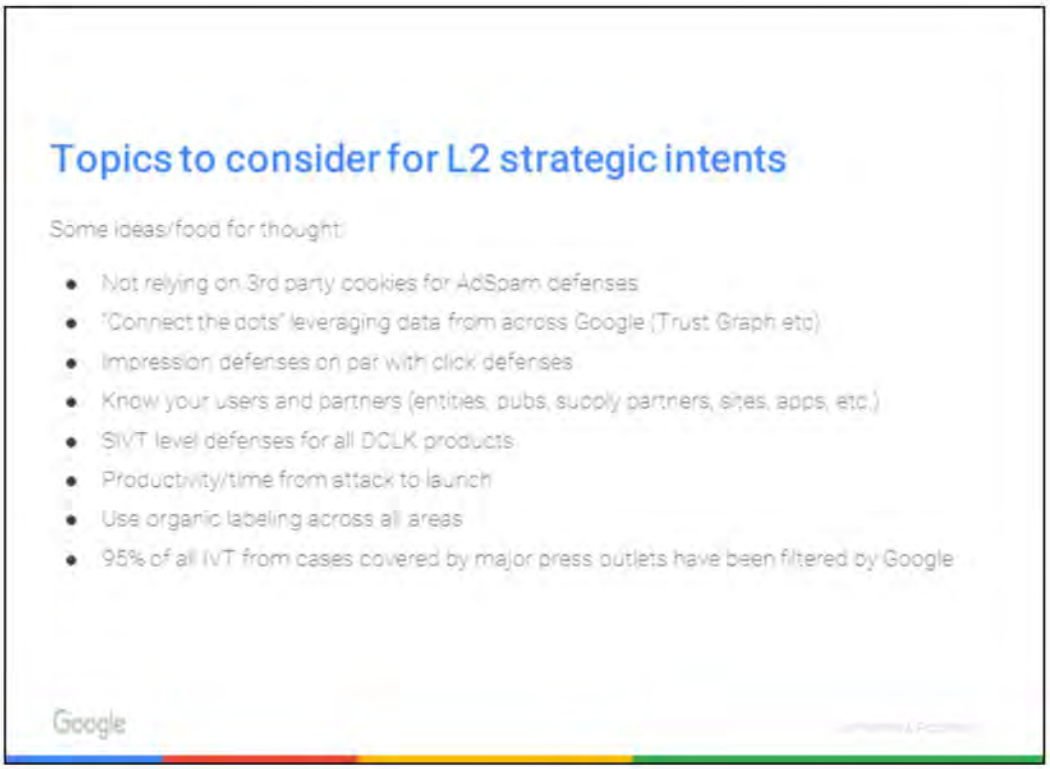
4) Protect Google by increasing IVT defenses and trust across the industry

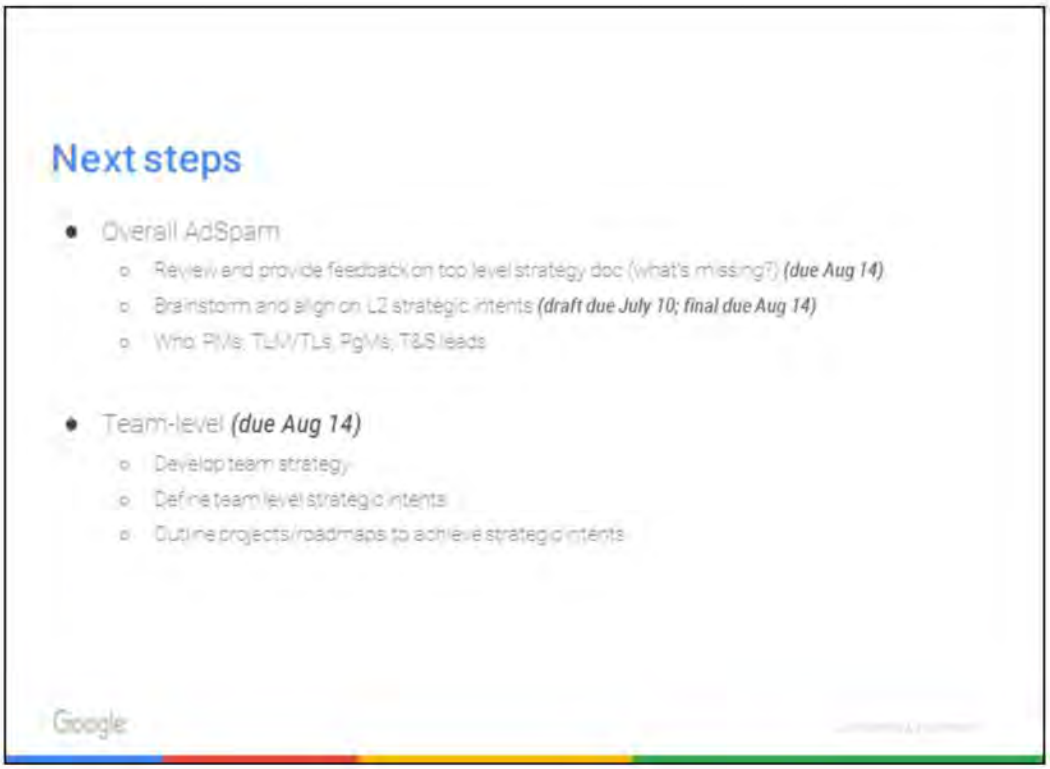
Description: In order to effectively fight and prevent IVT and ad fraud within Google, we need to increase IVT defenses and trust across the industry at large to minimize overall systemic risk.

Challenges:

- Sharing information without
  - leaking privacy sensitive data
  - giving the secrets to "bad guys"
- Hard to motivate an industry mostly focused on short-term revenue to invest for the long-term sustainability
- Lack of ground truth/effective advertising ROI metrics makes it hard to justify investments
- Monetary incentives not always aligned with sustained and effective IVT defenses

Google


Topics to consider for L2 strategic intents
Some ideas/food for thought:
Not relying on 3rd party cookies for AdSpam defenses
"Connect the dots" leveraging data from across Google (Trust Graph etc)
Impression defenses on par with click defenses
Know your users and partners (entities, pubs, supply partners, sites, apps, etc.)
SIVT level defenses for all DCLK products
Productivity/time from attack to launch
Use organic labeling across all areas
95% of all IVT from cases covered by major press outlets have been filtered by Google
Google

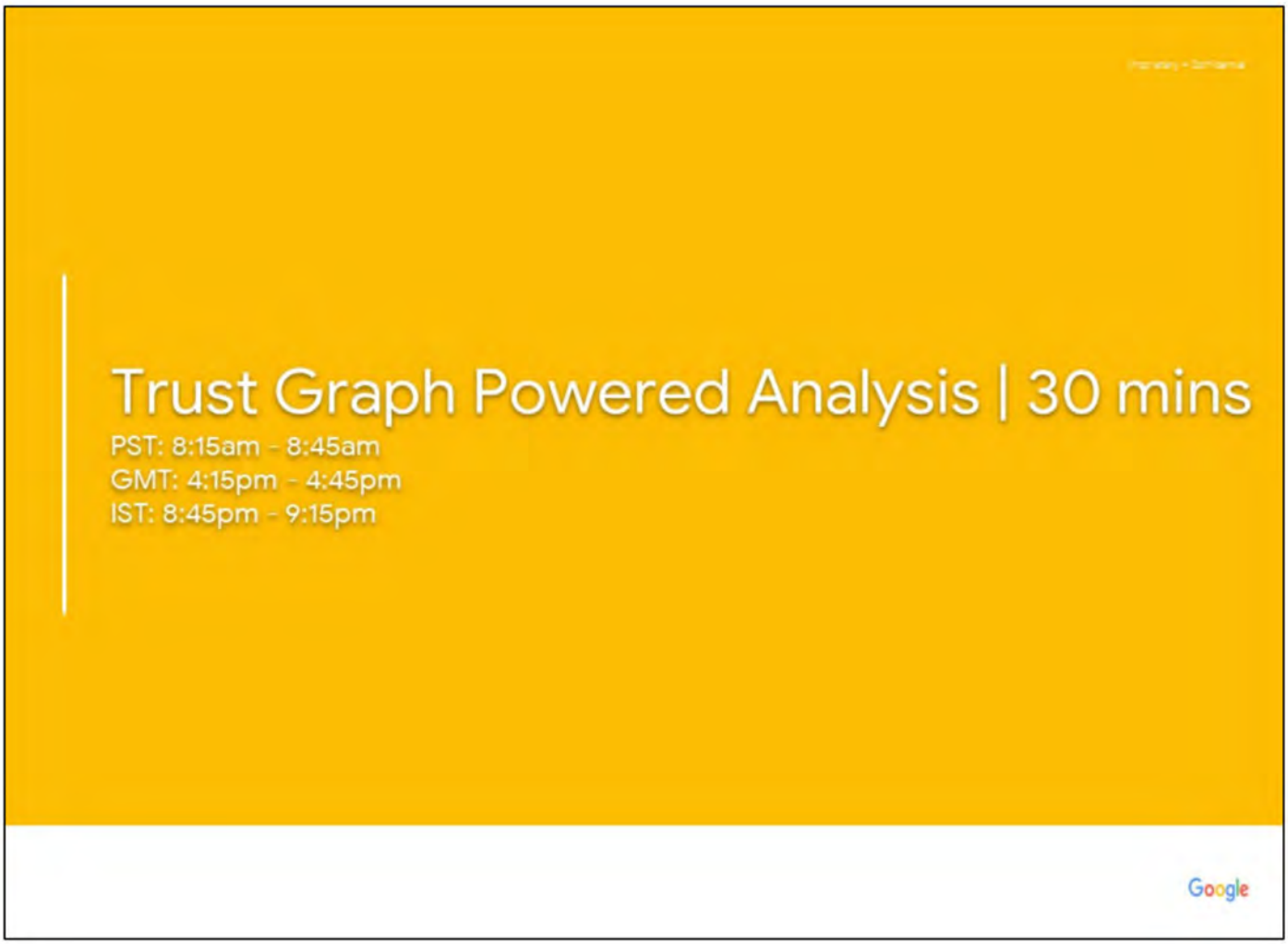

Next steps
Overall AdSpam
Review and provide feedback on top level strategy doc (what's missing?) (due Aug 14)
Brainstorm and align on L2 strategic intents (draft due July 10; final due Aug 14)
Who: PMs, TLM/TLs, PgMs, T&S leads
Team-level (due Aug 14)
Develop team strategy
Define team level strategic intents
Outline projects/roadmaps to achieve strategic intents
Google

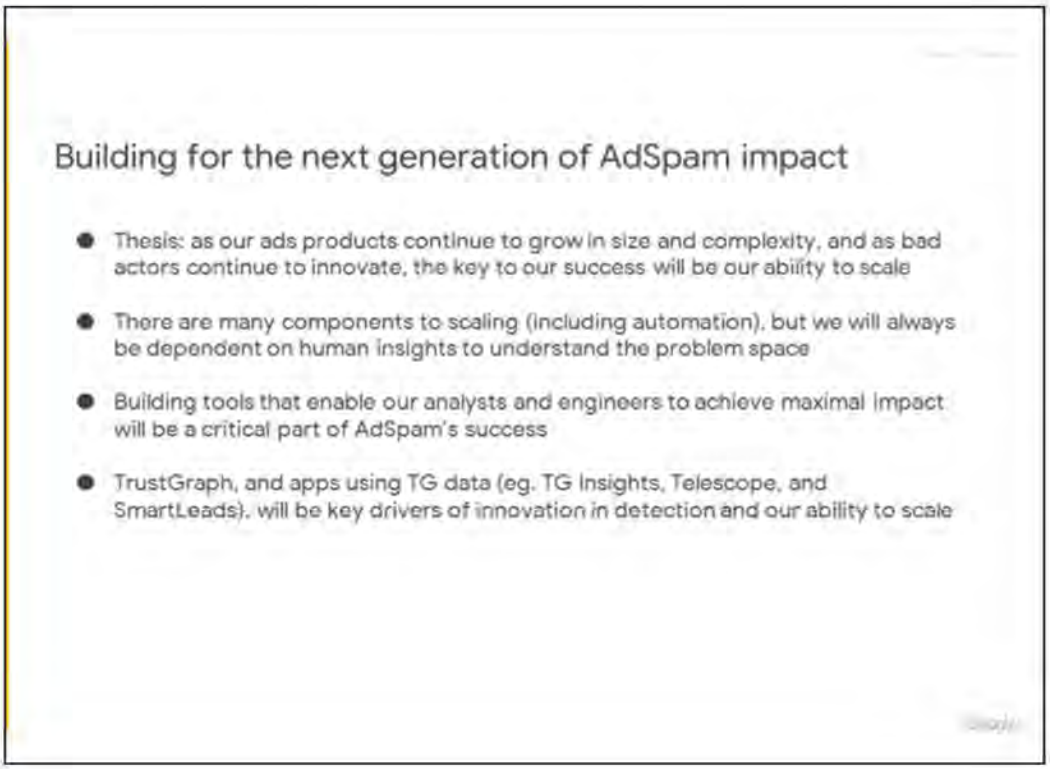
Break 15 mins

PST: 8:00am - 8:15am
GMT: 4:00pm - 4:15pm
IST: 8:30pm - 8:45pm

Next session: Trust Graph Powered Analysis

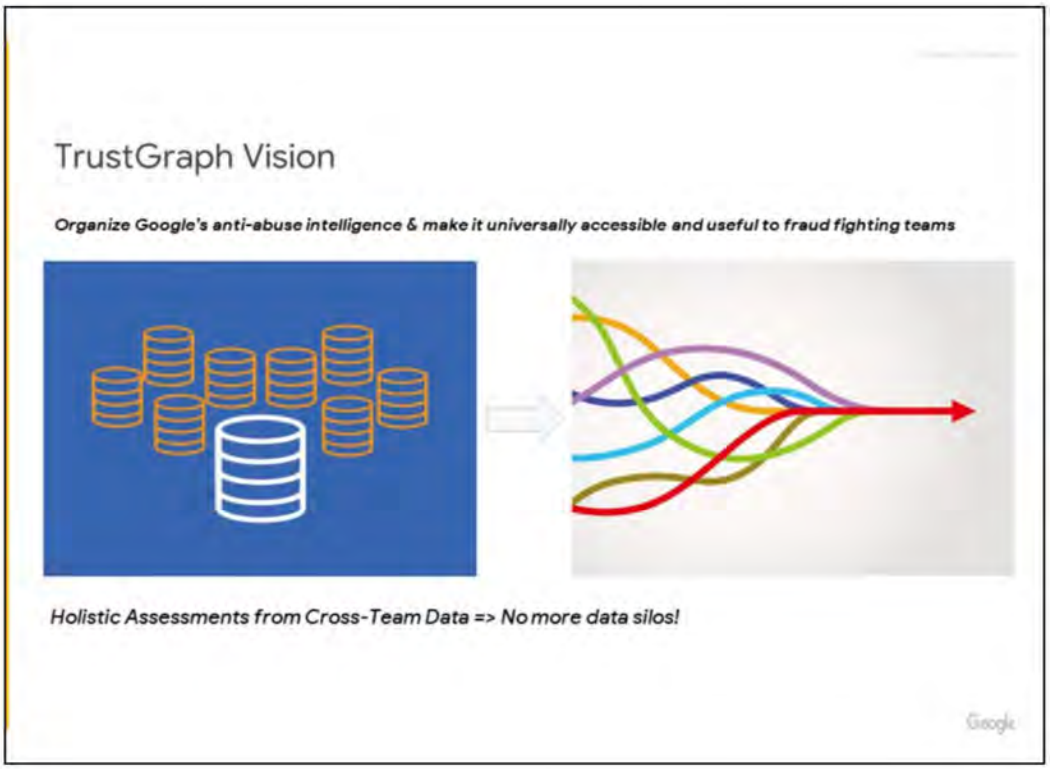
Google


Trust Graph Powered Analysis | 30 mins
PST: 8:15am - 8:45am
GMT: 4:15pm - 4:45pm
IST: 8:45pm - 9:15pm
Google

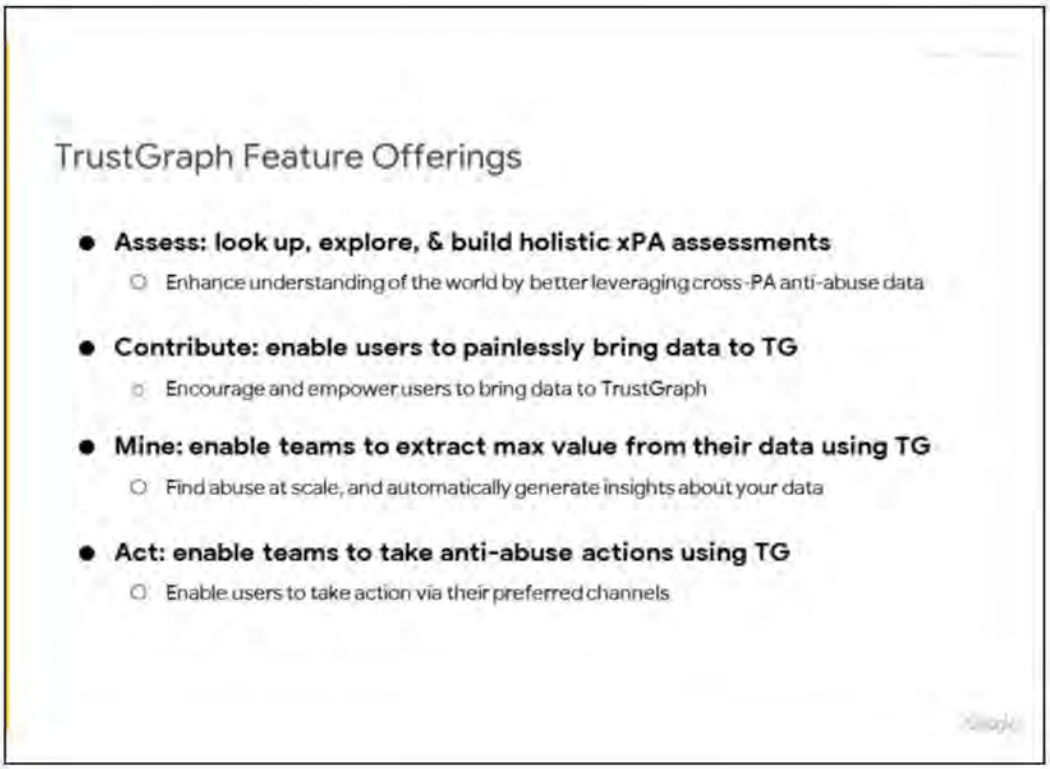


Speaker: Zack

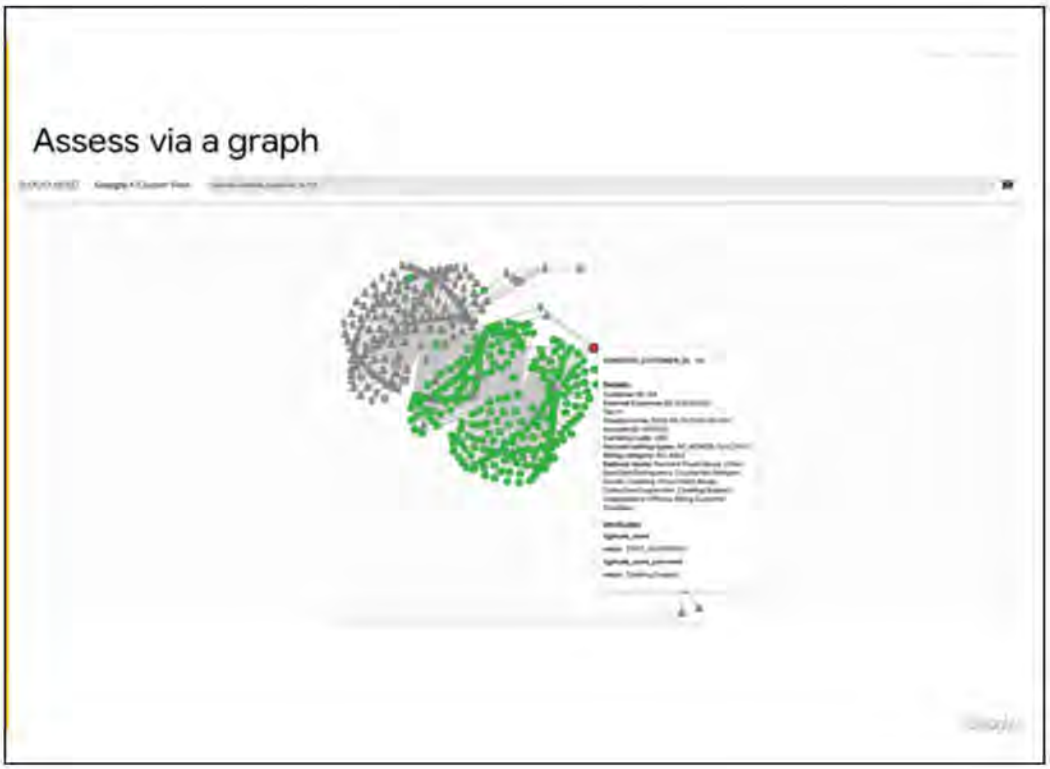
a) educate (feedback I keep hearing is folks dont know the vision/plan)
b) build enthusiasm (some selling on the future potential - but not overselling)
c) feedback / alignment



Speaker: Zack



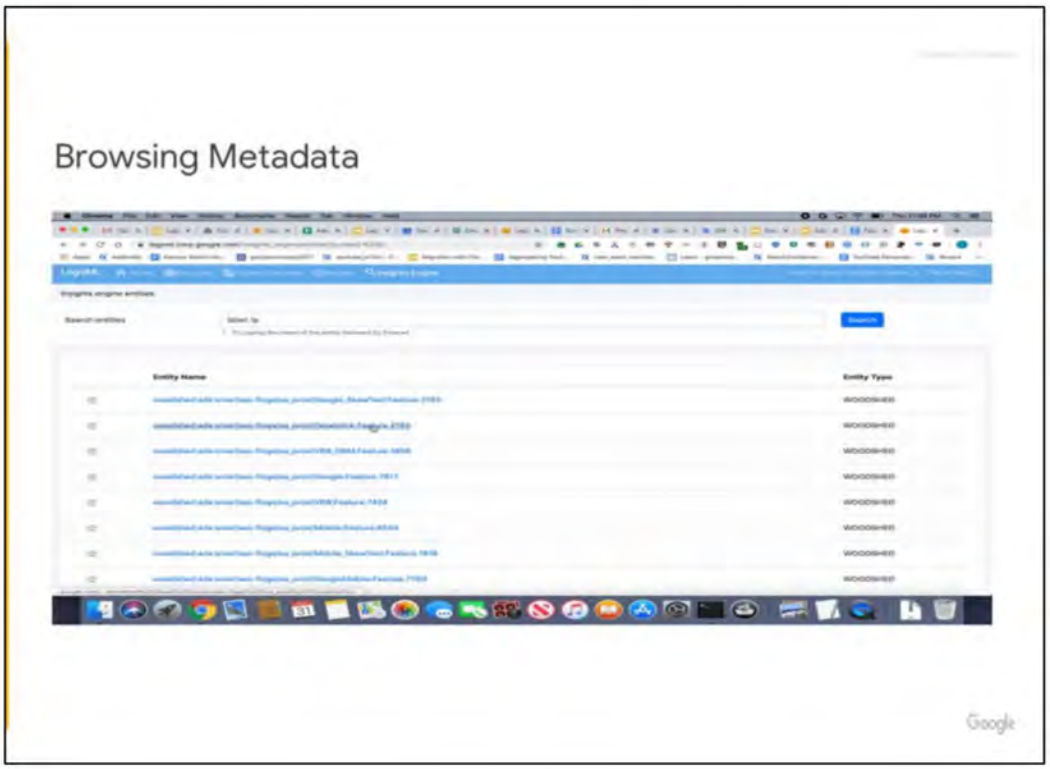
Speaker: Zack



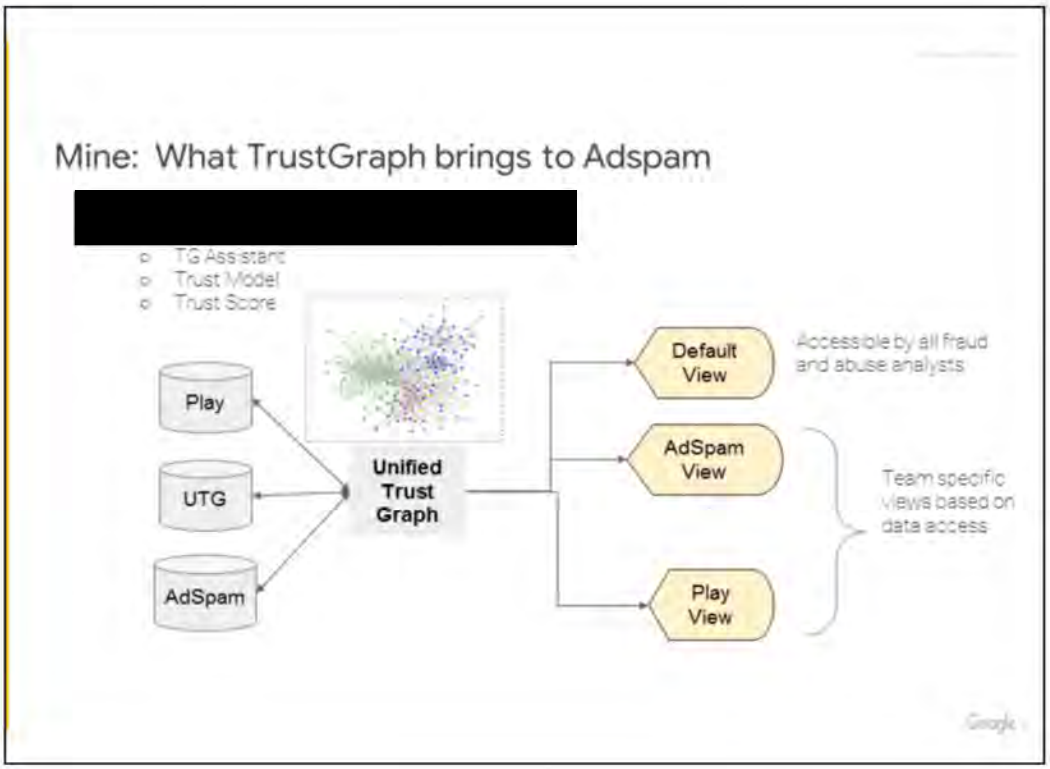
Talking points:
analysts can browse data using a combination of graphs and tables
mention that we have graph extraction (aka graph query language 0.5) as input
first version of this will be Smartmeter
would like to get feedback on the possibility of integrating this with other investigation tools

Id	Date	Text
1	06/22/2020 21:14:25	@xinzhao@google.com Please take a look at this slide and the next one. I plan to verbally say that these 2 UI would be combined at some point in the future in Smartmeter. Does this sound good to you? @zacharylf@google.com for a FYI _Reassigned to Xin Zhao_
1	06/22/2020 21:14:25	SG. This is indeed our plan. The graph help visualize the most relevant clusters/nodes, while tables provide detailed info and highlights from users' interpretation on signals.


Assess via a Table
SmartMeter
Google

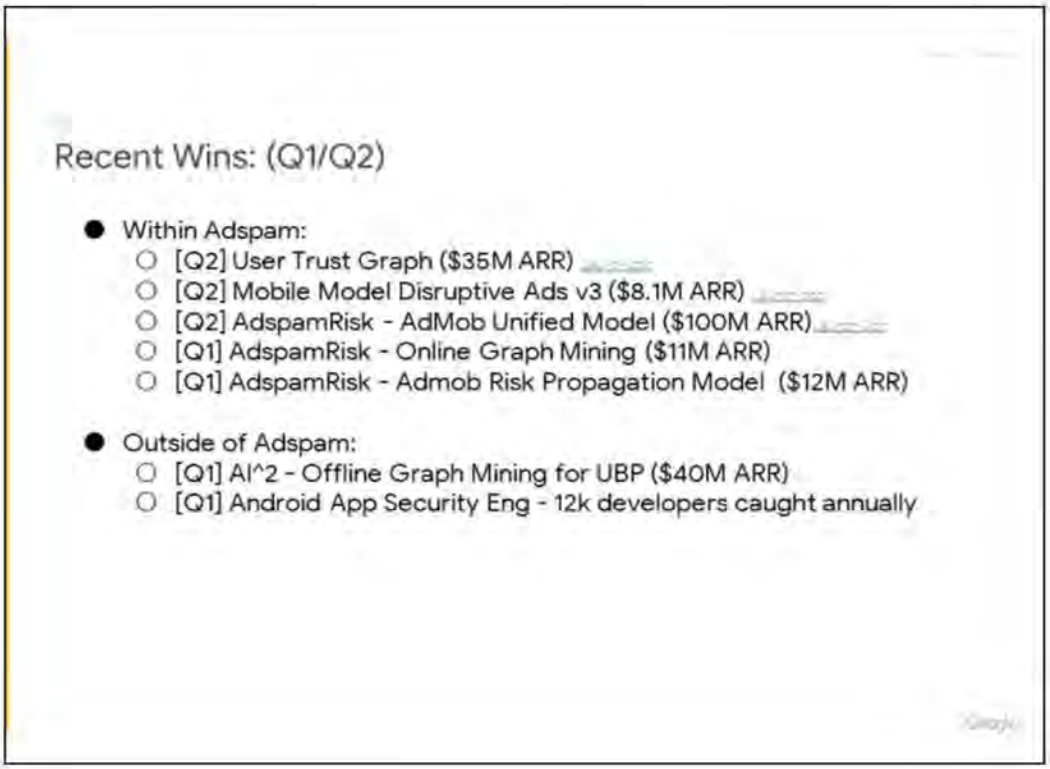


Might skip this if we don't have time



[redacted]

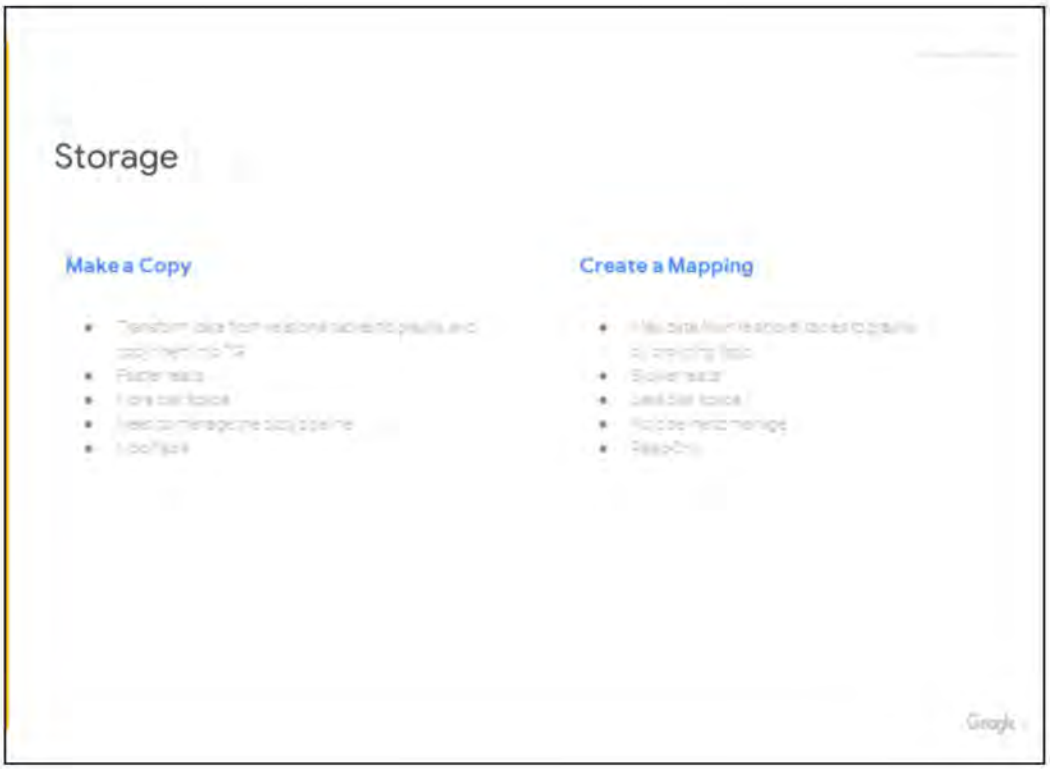
Unified Trust Graph -> Trust Model -> Trust Score



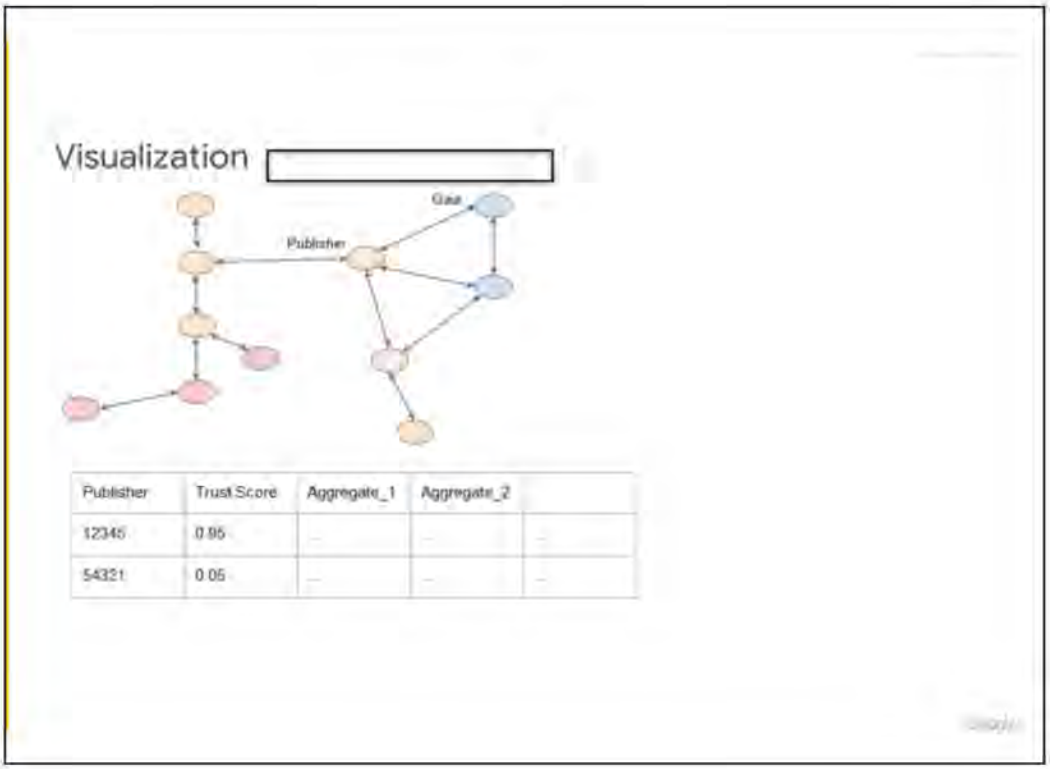
There are some launches here that we could include.

Id	Date	Text
2	06/22/2020 18:10:38	@kalpa@google.com
3	06/22/2020 21:17:47	Just added ones from here: https://docs.google.com/document/d/1AN7Ht8j6rwtGVUYwZe0la2HI8fCbsSzF20NWHdcqs2Y/edit#
1	06/22/2020 21:26:21	I am unable to edit but we should add these launches too - https://docs.google.com/presentation/d/1z7iyGGJEL8Kf9Rb1lly7VwTbgUH1OH568SlwM0z6BTc/edit#slide=id.g7e4601850f_1_0
1	06/22/2020 23:34:41	+hsiaosu@google.com Do you have any material on early wins for UTG and AdSpam Risk we can highlight here?
4	06/22/2020 23:34:41	I filled out a few more from here: go/tg-impact&engagement-tracker

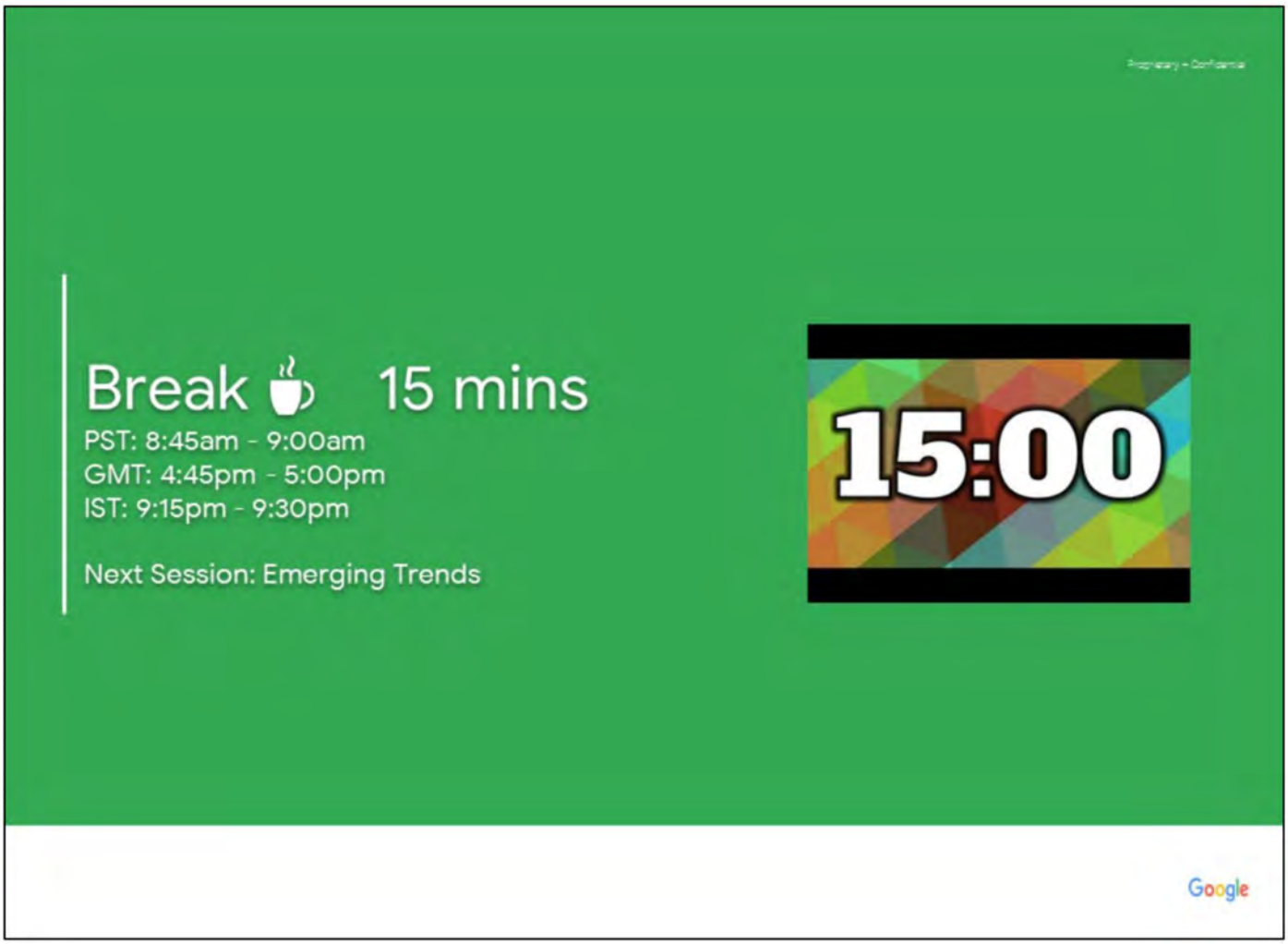
Simplify this slide, stress that we'll make privacy easier.

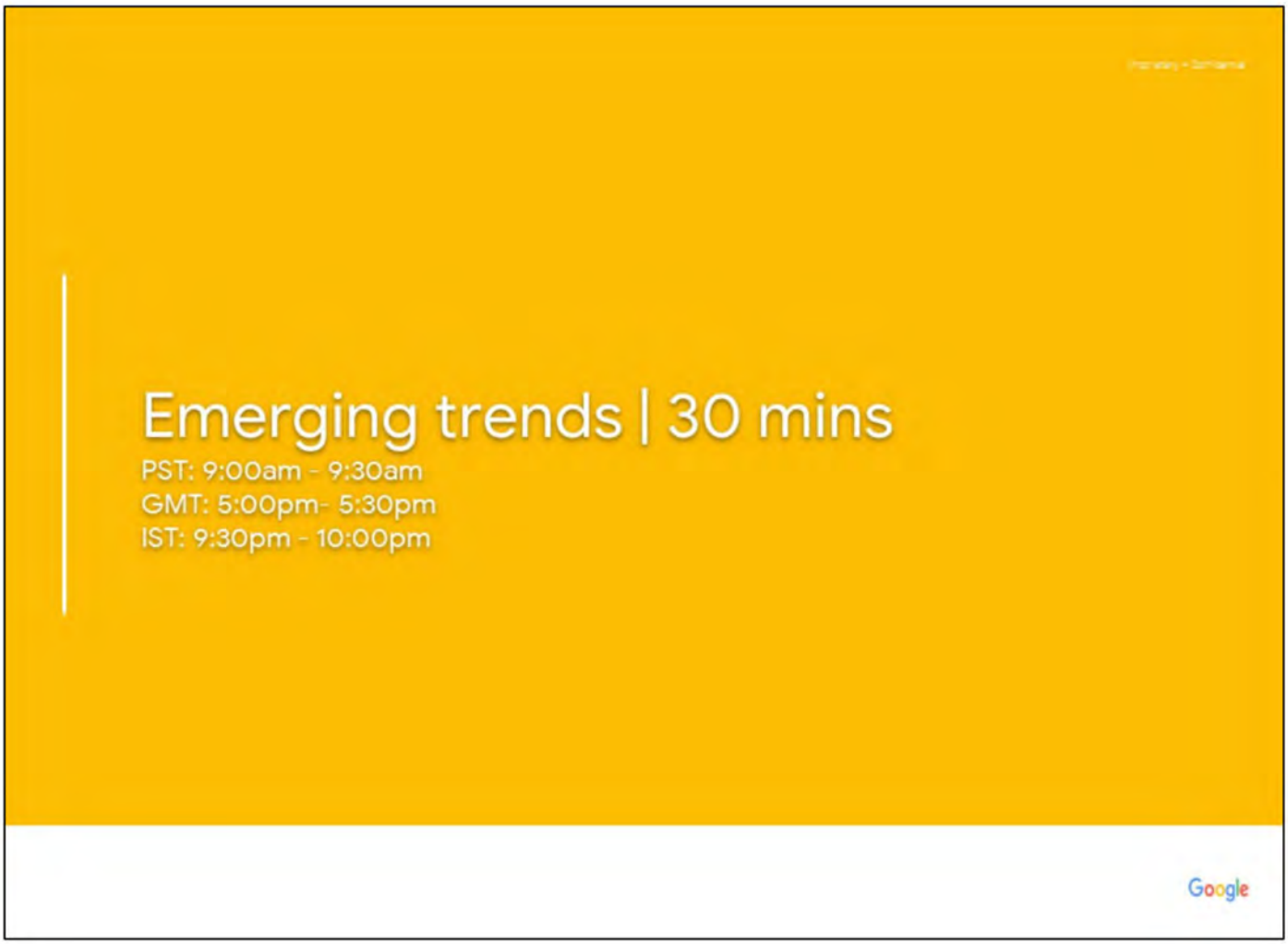


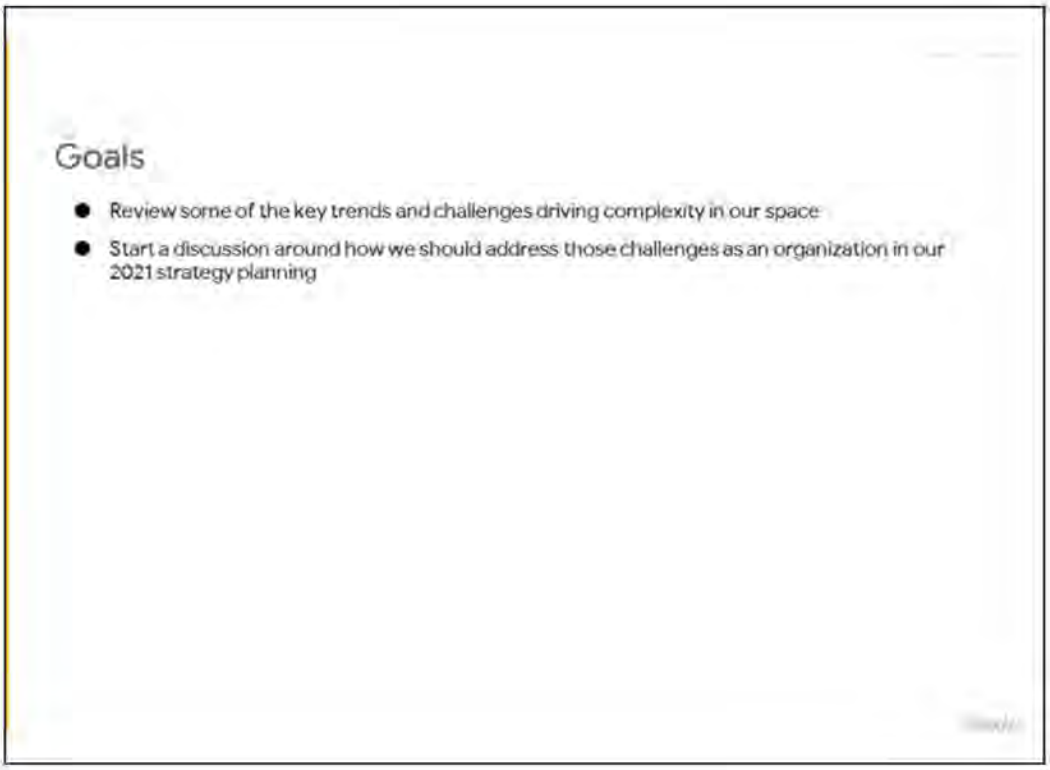
Skip this



Talking points:
analysts can browse data using a combination of graphs and tables
mention that we have graph extraction (aka graph query language 0.5) as input
first version of this will be Smartmeter
would like to get feedback on the possibility of integrating this with other investigation tools


Break 15 mins
PST: 8:45am - 9:00am
GMT: 4:45pm - 5:00pm
IST: 9:15pm - 9:30pm
Next Session: Emerging Trends
15:00
Google


Emerging trends | 30 mins
PST: 9:00am - 9:30am
GMT: 5:00pm- 5:30pm
IST: 9:30pm - 10:00pm
Google



The goal of this session is to seed a conversation about the big picture trends and challenges facing AdSpam as we go about our 2021 planning.

This isn't a TED talk, I don't have a crystal ball, but hopefully this will start a useful discussion and help us frame our annual strategies in a way to address some of these challenges.

AdSpam operates in a really complex space. Externally, the digital ads ecosystem is growing, evolving, and maturing - reaching new forms of media.

Internally, Google's variety of businesses, infrastructure, and organizational structure is extremely complex in its own right.

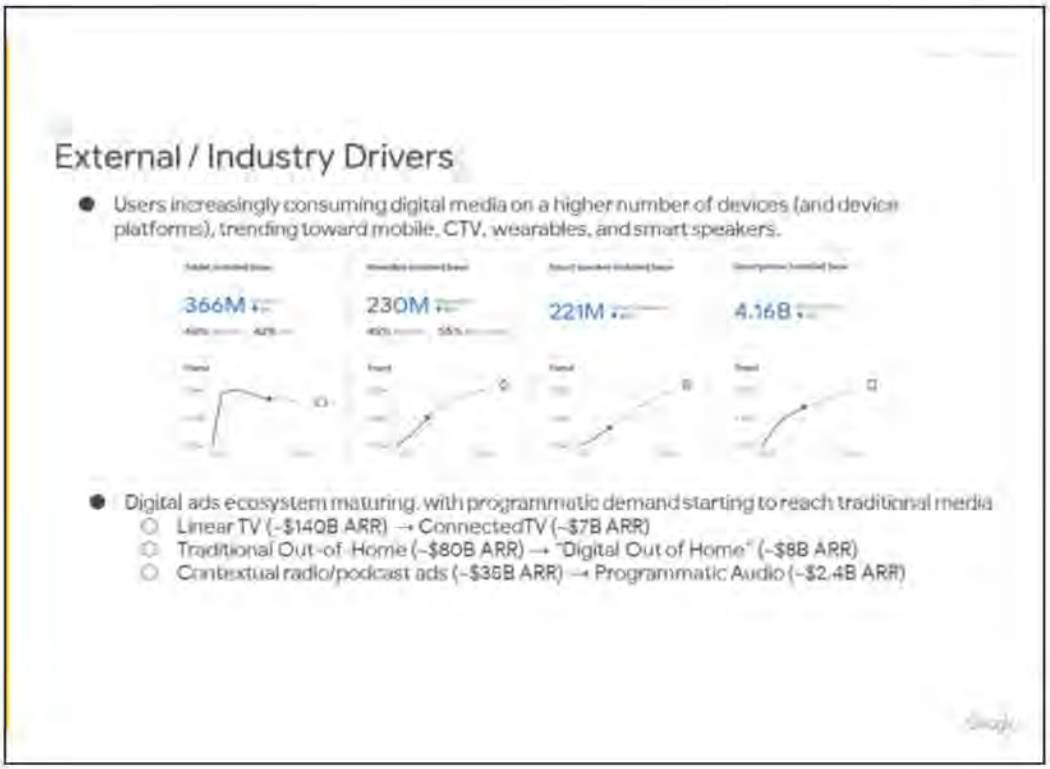
We've developed ways to help us navigate complexity (like alignment), and address it more structurally through standardizing our integration requirements, and innovating in our analysis methodologies and infrastructure (eg, ASML, TrustGraph, Organic Labeling).

This has helped us be relatively successful in both supporting new product requirements and feature requests, and scaling our defenses across Google's wide array of businesses, as part of our "standard solution"

The emerging trends that are driving the complexity we deal with on a daily basis, originating both internally and externally to Google, are pointing to an expansion in variety and diversity of online ad experiences for users and platforms where they happen.

As a result, we're increasingly seeing requests fall outside of these standard processes and solutions, requiring custom work and constant alignment.

As we go through strategic planning, how can we get ahead of these trends? Are there any asymmetric bets we can invest in in 2021?



Starting with external trends:

The ads ecosystem follows user behavior. Increasingly, users are engaging with ad supported content across a higher number and wider variety of devices. We've all heard about the shift from desktop to mobile, and now we're seeing the beginnings of a shift to wearables, smart speakers, and connected TV devices. New devices, ad formats, attack vectors, signals and collection mechanisms, all require additional attention from AdSpam.

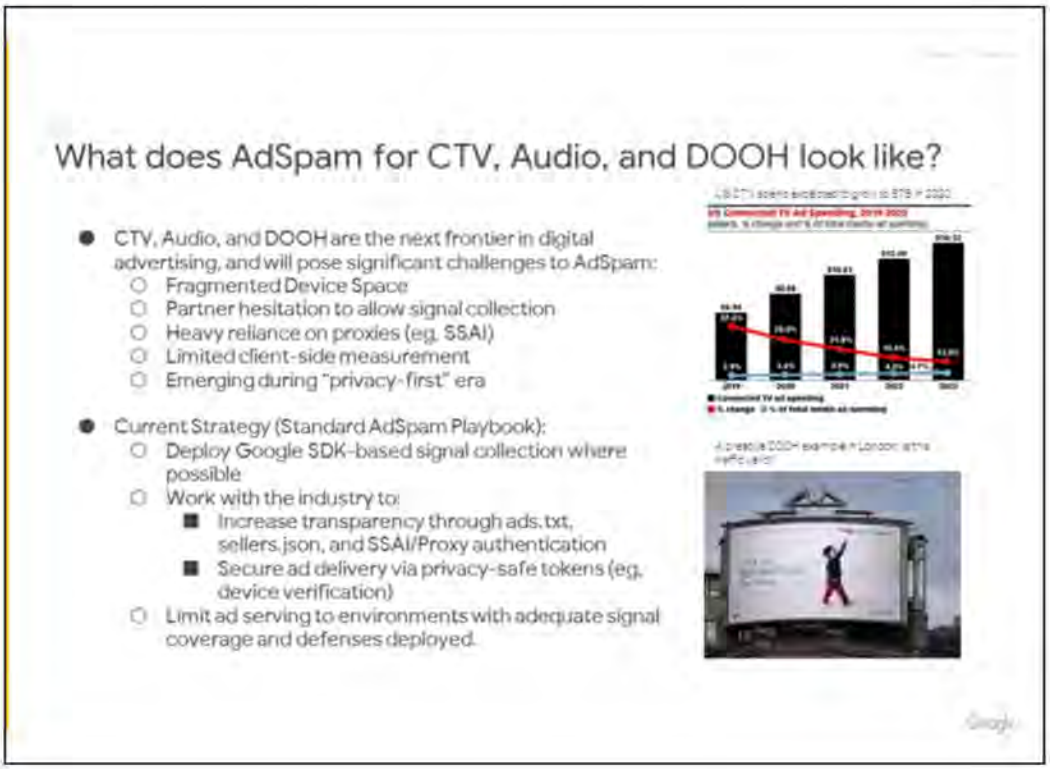
The second trend to call out here is similar - as the digital ads ecosystem matures, we're starting to see a shift in "traditional" ad spend moving to digital, and from digital to programmatic. While CTV, DOOH, and Audio are all multi-billion-dollar markets already, look at how much is still spent on their traditional siblings -- over $250B!

Not all of this will move to digital, and what does isn't going to move all at once, but I think this does at least hint that we'll continue to see continued growth in these new areas for the years to come.

Within Google, we're increasingly seeing an effort to consolidate ad format and inventory offerings, to allow advertisers to run the same ad in more places. For example, if you look at recent developments in the YouTube app, you'll notice AFS ads, Shopping ads, and Feed ads have been incorporated into the Home and Search pages.

At the same, innovation in formats and billing models are challenging some of AdSpam's assumptions around expected user interactions, metrics, and even logs and event-hierarchies.

For example, in immersive formats on Search such as Shopping, Local Services, or Maps, we often log multiple clicks for each ad - the first is to open the immersive, the second is the ad click. Enhanced Conversions have found that their requirements can't be met with the AdEvents logs.



By way of example: CTV, Audio, and DOOH are the "next big thing", and incorporate a lot of these trends.
[DEFINE THE TERMS]

We're the furthest along in our defense of CTV, and so far, we've tried to apply the standard AdSpam playbook.

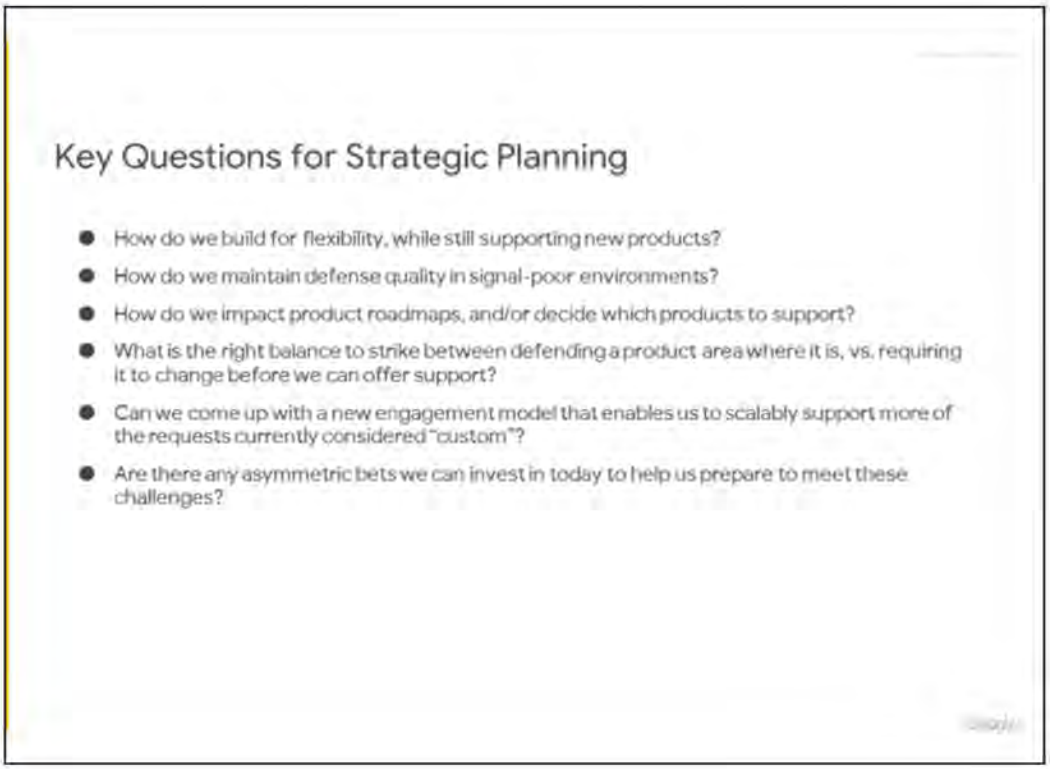
As we expand down the long-tail of CTV devices, and into smart speakers and billboards, do we need a different approach? How does the definition of IVT change for these formats?

Recent shifts if Mobile app advertising and related abuse vectors are also rapidly changing, and challenging us in unique ways - I believe Zack is going to cover some of these in a future session.

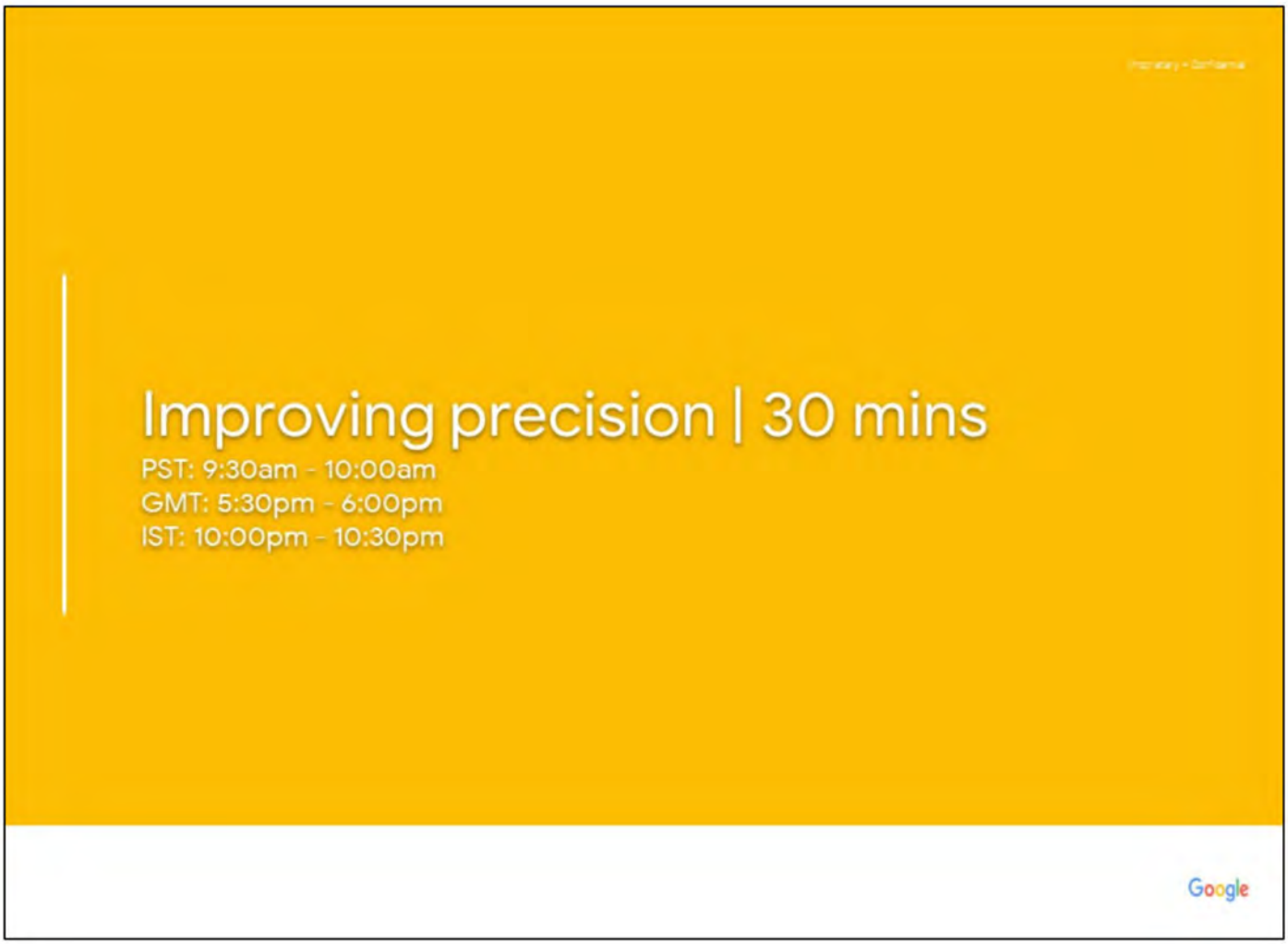
So how do these trends affect AdSpam?

These trends are pointing to two new business requirements that we'll need to find a way to support.

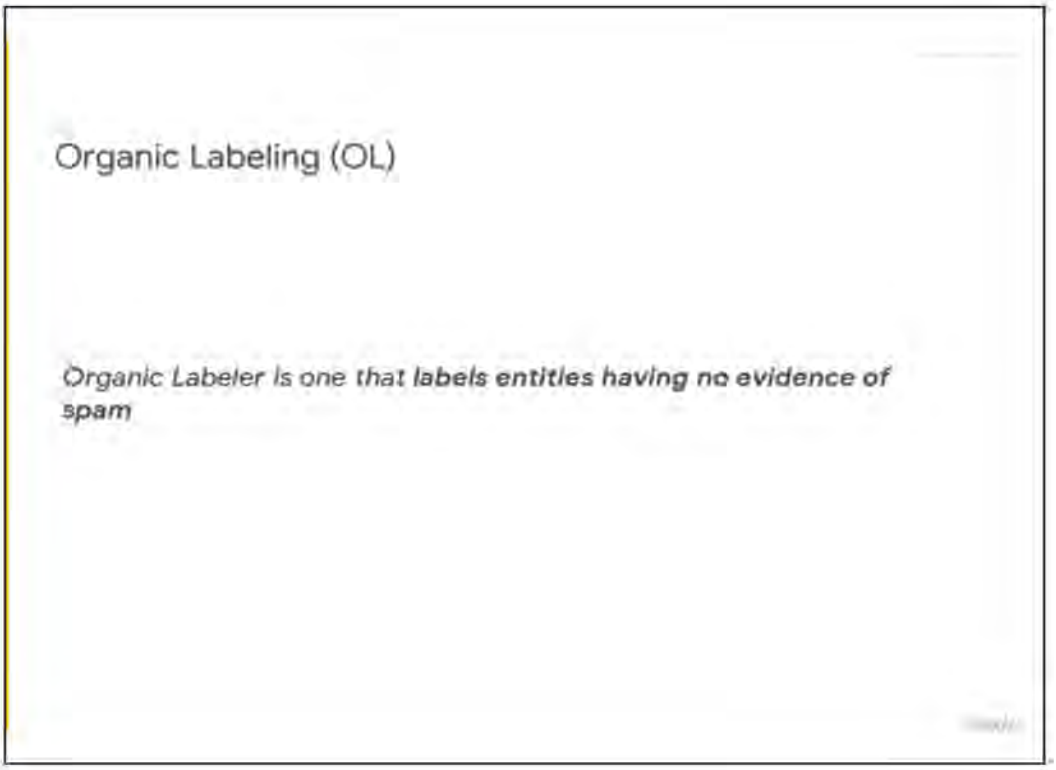
And becoming flexible enough to support those new requirements won't be easy.



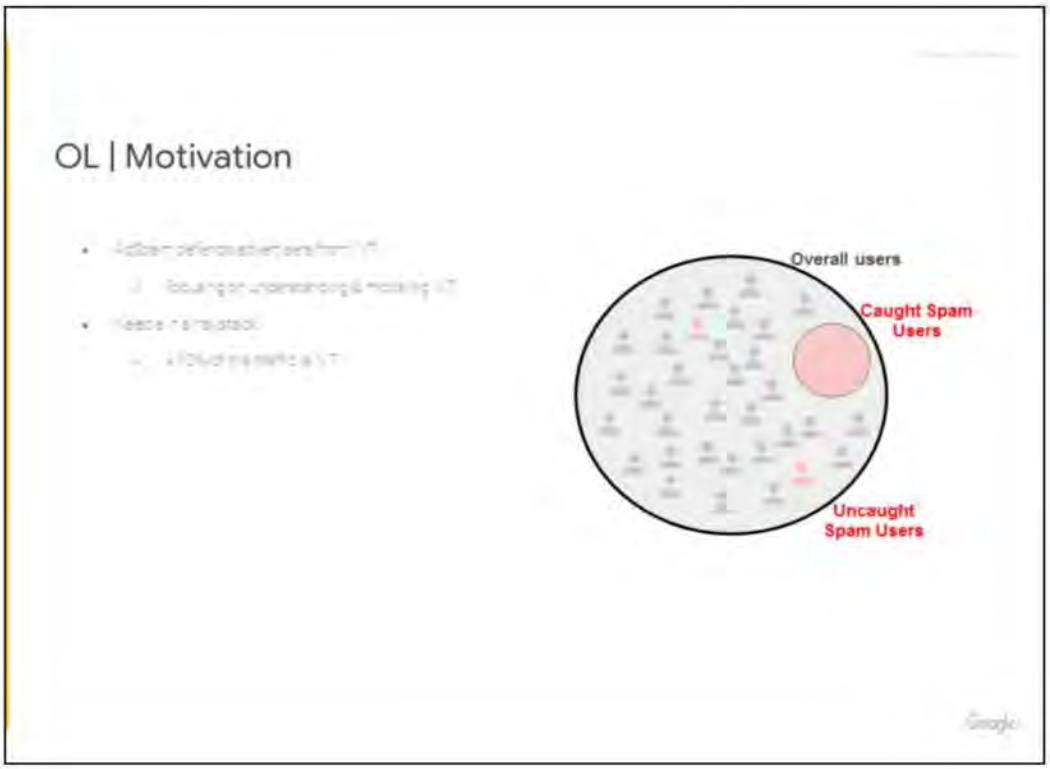
So as we go through this strategic planning summit and related exercises, I think there are a few key questions that I hope we can keep in the back of our minds.


Improving precision | 30 mins
PST: 9:30am - 10:00am
GMT: 5:30pm - 6:00pm
IST: 10:00pm - 10:30pm
Google

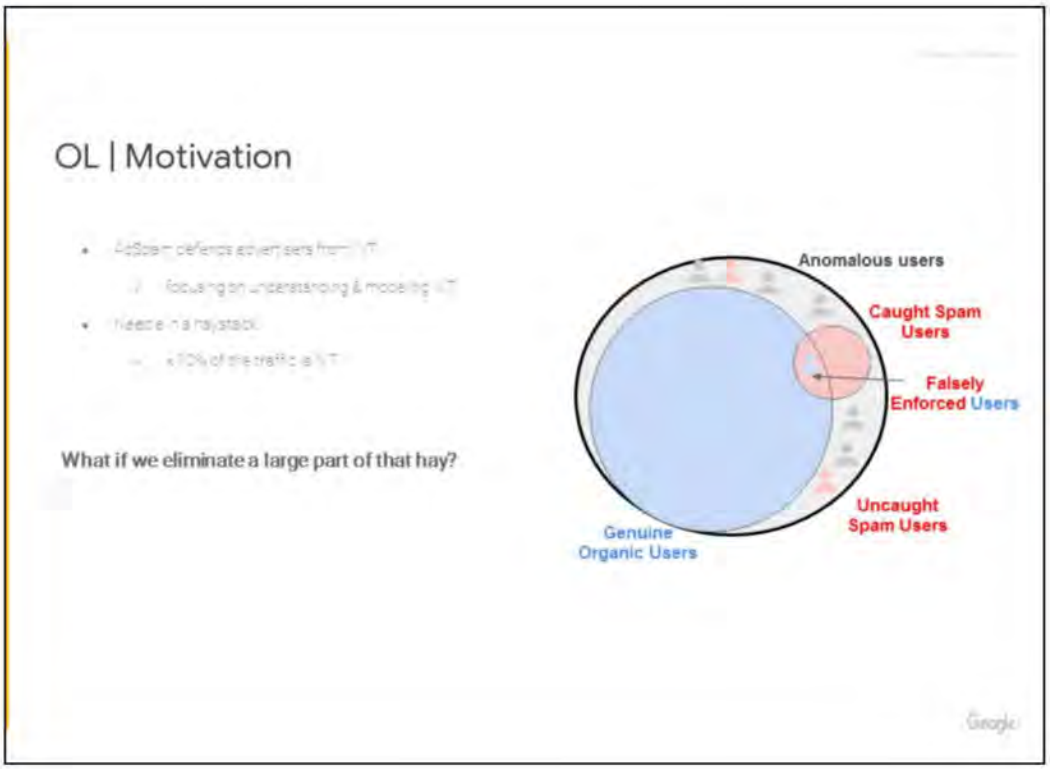
Id	Date	Text
1	06/16/2020 22:03:35	@spacemanspiff@google.com @atali@google.com
1	06/16/2020 22:03:35	@sulabha@google.com I think you had a couple slides to share too



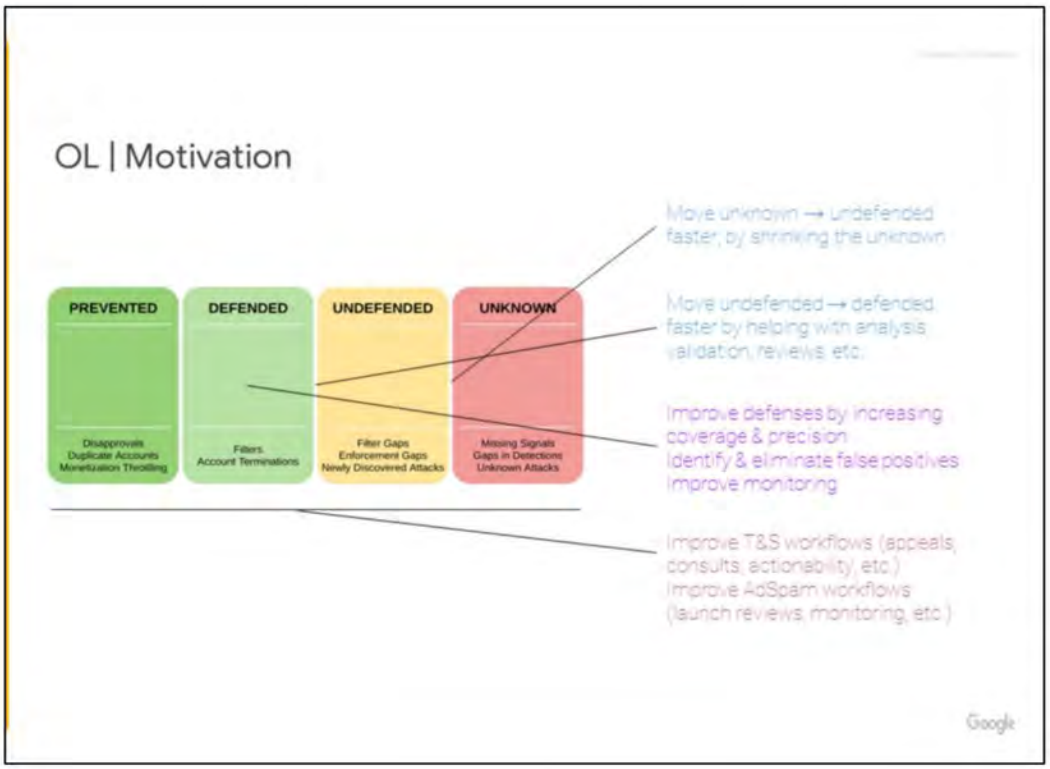
Slides heavily stolen from a bunch of different slide decks by rahulmah@.



Uncaught spam << 0.5%.



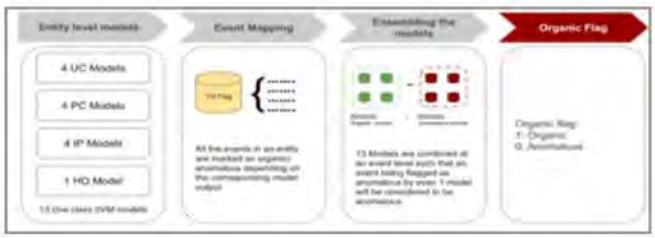
Uncaught spam << 0.5%.


OL | Motivation
PREVENTED
DEFENDED
UNDEFENDED
UNKNOWN
Disapprovals
Duplicate Accounts
Monetization Throttling
Filters
Account Terminations
Filter Gaps
Enforcement Gaps
Newly Discovered Attacks
Missing Signals
Gaps in Detections
Unknown Attacks
Move unknown → undefended faster, by shrinking the unknown
Move undefended → defended faster by helping with analysis validation, reviews, etc.
Improve defenses by increasing coverage & precision
Identify & eliminate false positives
Improve monitoring
Improve T&S workflows (appeals, consults, actionability, etc.)
Improve AdSpam workflows (launch reviews, monitoring, etc.)
Google

OL | s-spam

- Launched in Q1 2020
  - One Class Support Vector Machines (OCSVM) - sklearn
  - Unsupervised (no ground truth)
  - Mimics non-vl.ook for organic-ness in manual reviews
    - Learns the majority class function (majority of our traffic is organic) and predicts what is similar to the majority class
  - Labels available in vlogEvents and GoldStore

[redacted]



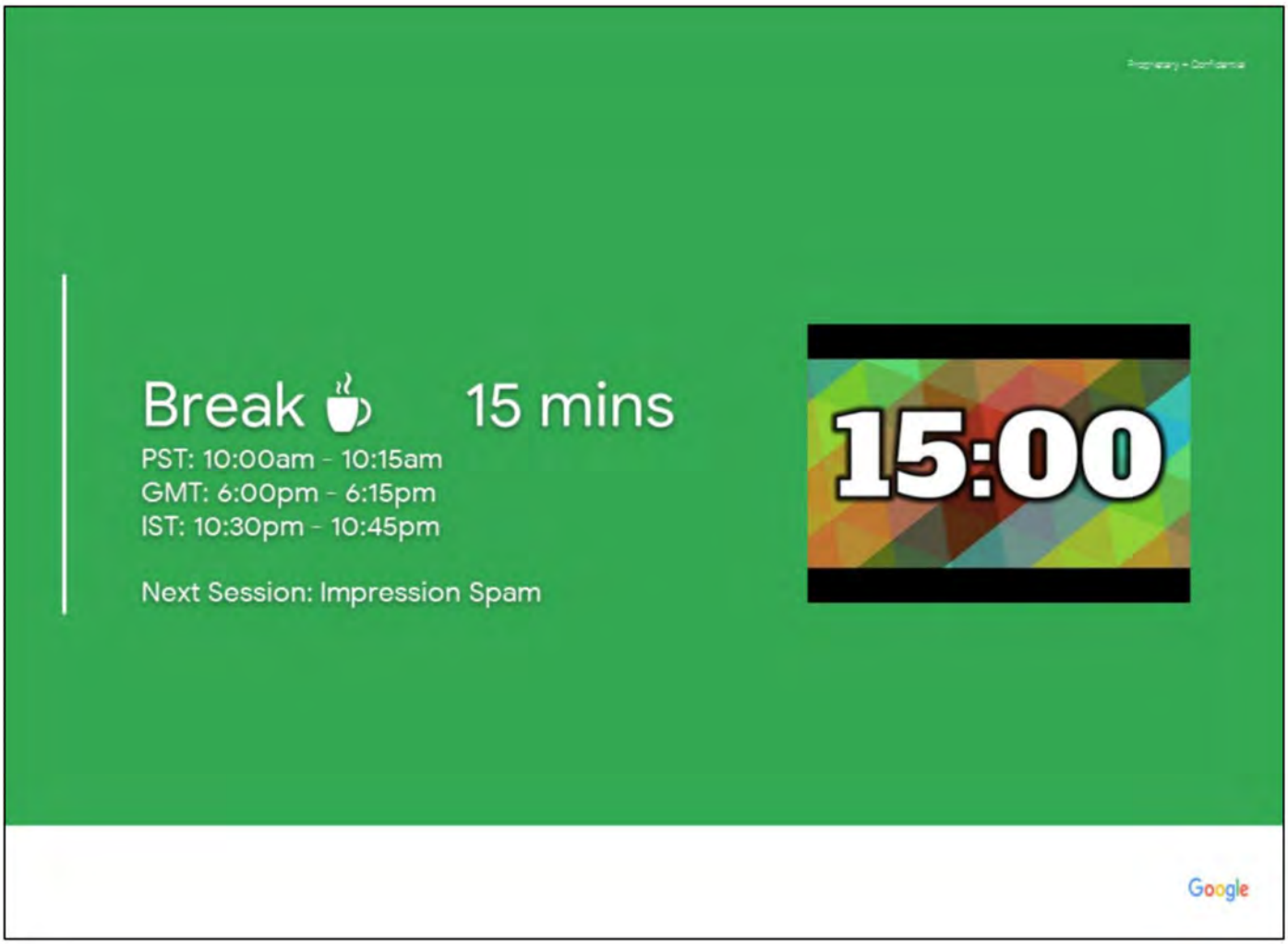
Google

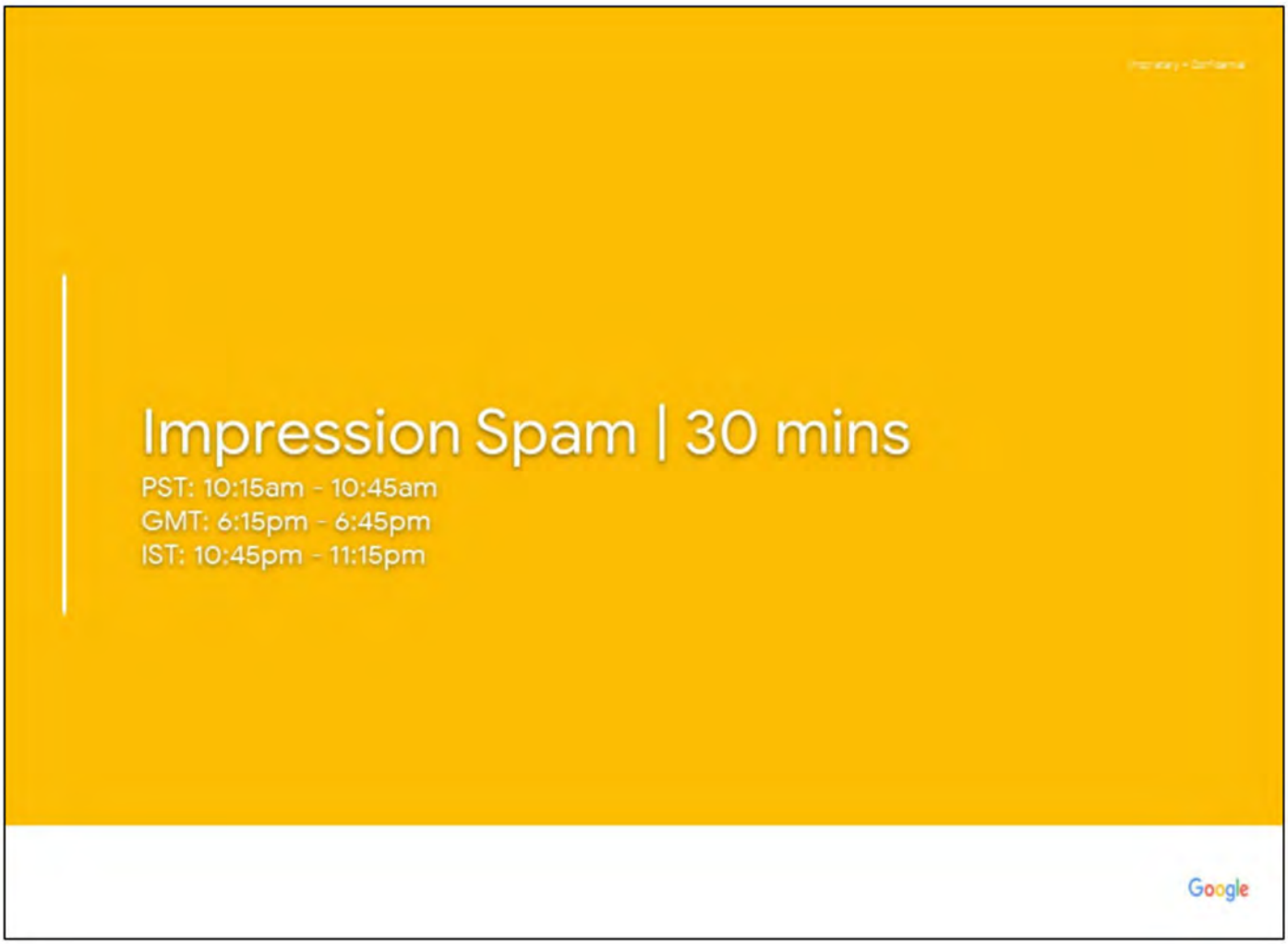

OL | Benefits so far
Machine Learning
Revenue Saving
Spam Detection
Process Optimization
Impact till date
2020 Target
~60% Labeled Clicks for Richer ML Experience so far
~63% Labeled Clicks for Richer ML Experience
$50M/Year of Revenue Saving to Google realized/ near realization
$100M/Year of Revenue Saving to Google
$50M/Year of Efficient Spam Detection so far
$55M/Year of Efficient Spam Detection
~1 FTE Saving through Process Optimization
~1.5 FTE Saving through Process Optimization
•Labels ~37% more than ASI/ML's LGP
•Significantly improved Precision and Recall
•Apollo^2 LGP Filter replacement (~$30K/day revenue savings)
•RR = 12, 15B & 97 Turn Down Insights (~$100K/day)
•Protective exclusions in our ASI/ML pDD filter (~$15K/day)
•Increases ASI/ML coverage on Search by $60.6M ARR
•more $29.4M ARR with DQ = 0.09
•Incremental $5.8M ARR with DQ = 0.995
•Consults
•Manual reviews (PD integration)
•Proactive overfiltration detection dashboard
Google

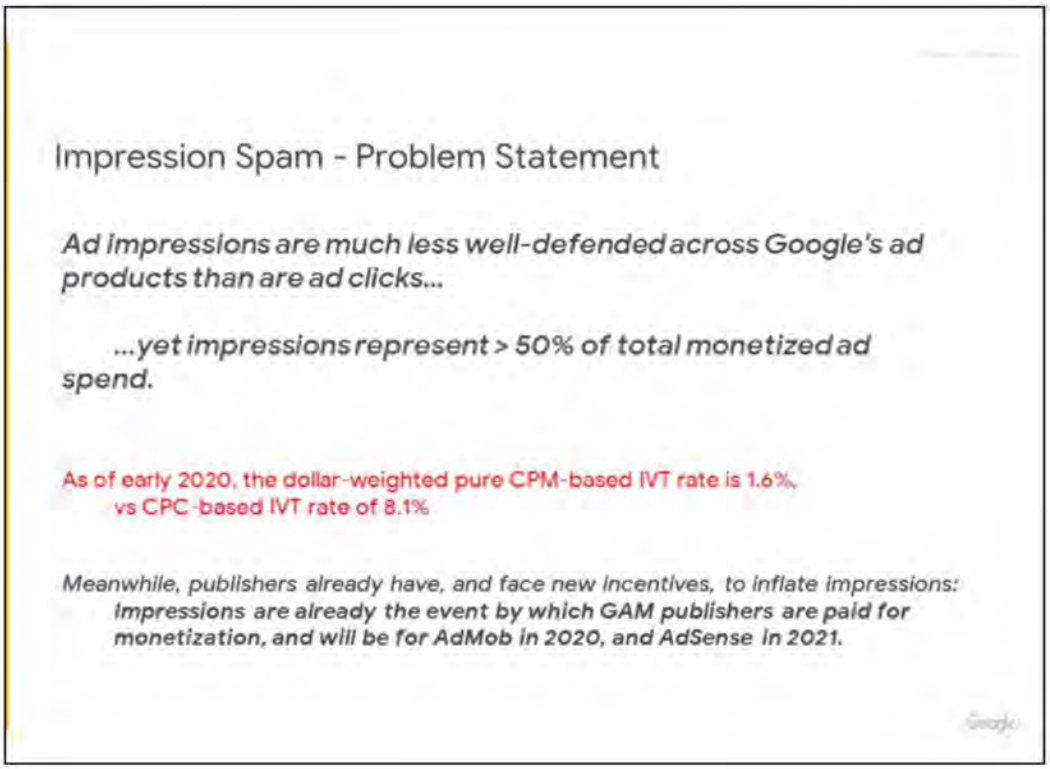
rahulmah: As per OL insights we know that at least 30-40% FPs are in form of collateral damage and turn downs are not the complete solution? We expect this to be the case across verticals as well.


OL | There's more

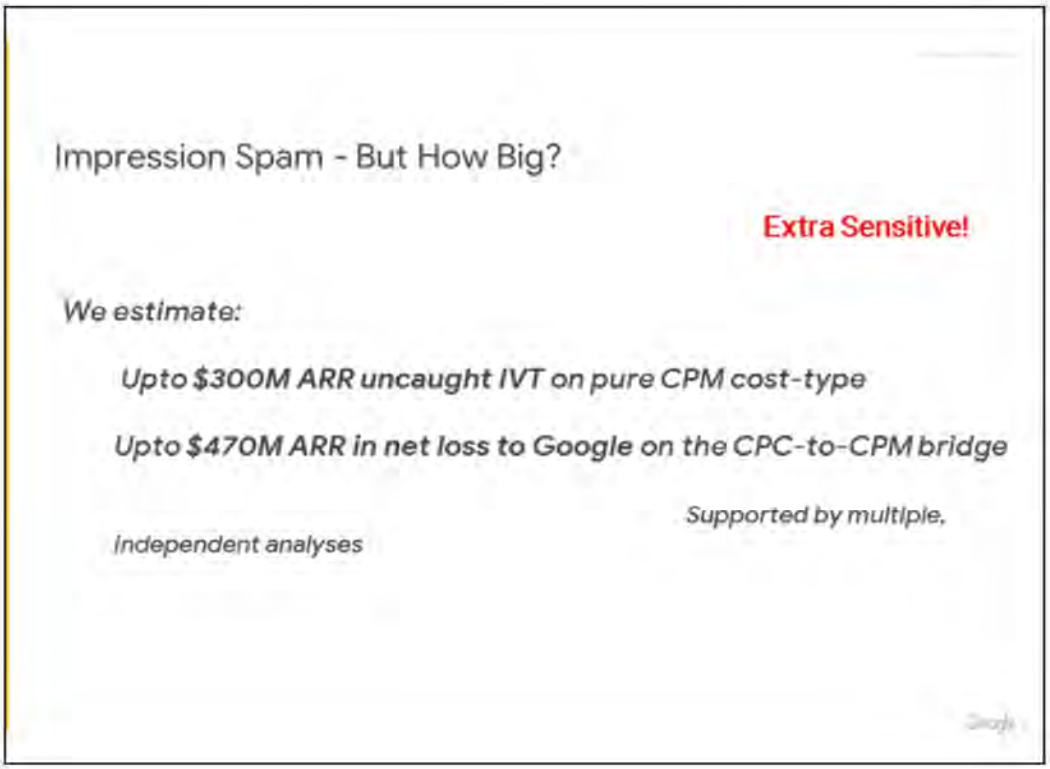

OL | Takeaways


Break
15 mins
PST: 10:00am - 10:15am
GMT: 6:00pm - 6:15pm
IST: 10:30pm - 10:45pm
Next Session: Impression Spam
15:00
Google

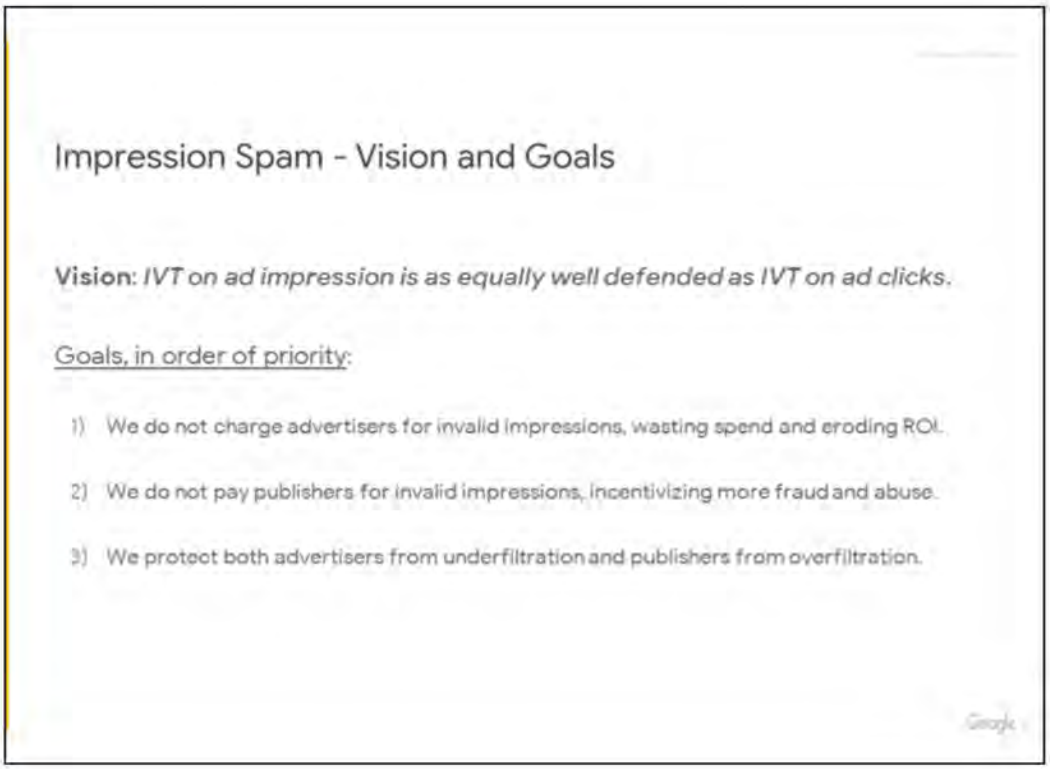

Impression Spam | 30 mins
PST: 10:15am - 10:45am
GMT: 6:15pm - 6:45pm
IST: 10:45pm - 11:15pm
Google



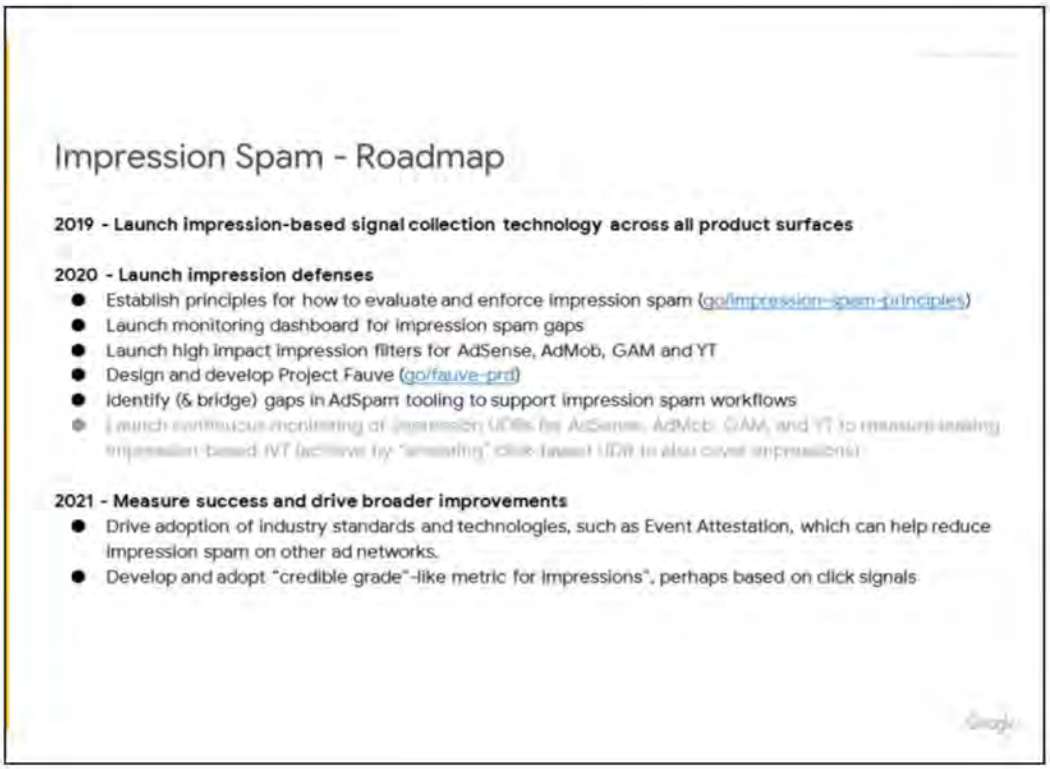
Speaker: Zack



Speaker: Zack



Speaker: Zack



Impression Spam - Roadmap

2019 - Launch impression-based signal collection technology across all product surfaces

2020 - Launch impression defenses

- Establish principles for how to evaluate and enforce impression spam (go/impression-spam-principles)
- Launch monitoring dashboard for impression spam gaps
- Launch high impact impression filters for AdSense, AdMob, GAM and YT
- Design and develop Project Fauve (go/fauve-prd)
- Identify (& bridge) gaps in AdSpam tooling to support impression spam workflows
- Launch continuous monitoring of impression UEIs for AdSense, AdMob, GAM, and YT to measure leaking impression-based IVT (achieve by "smearing" click-based UEI to also cover impressions)

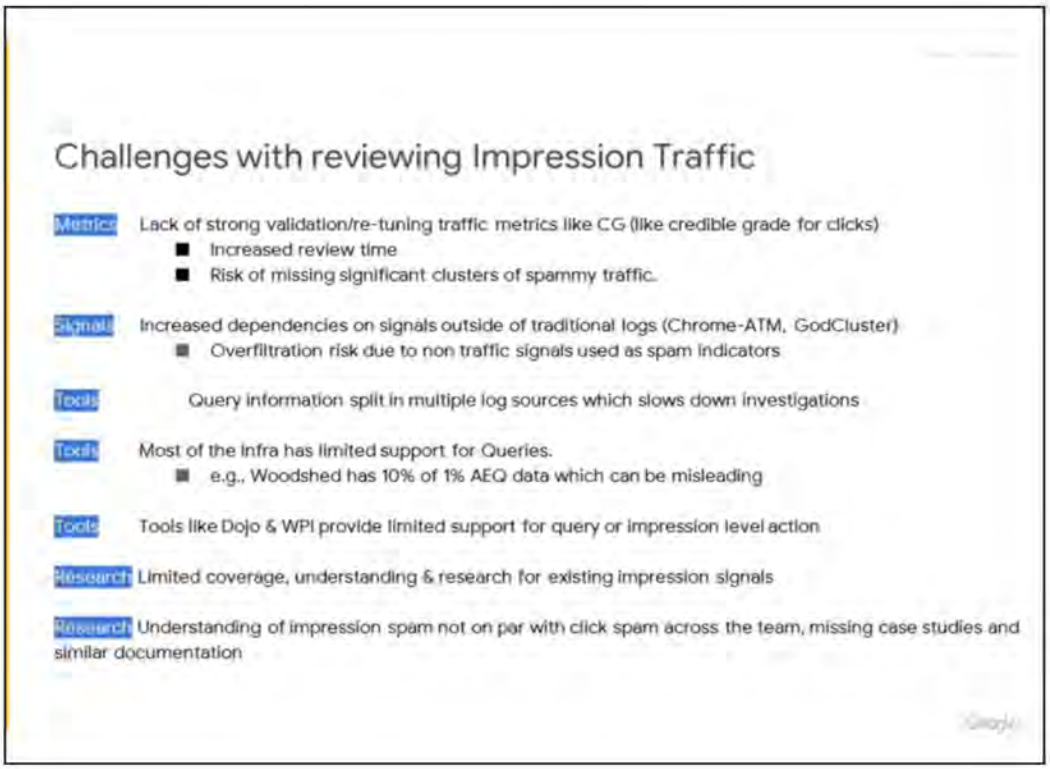
2021 - Measure success and drive broader improvements

- Drive adoption of industry standards and technologies, such as Event Attestation, which can help reduce impression spam on other ad networks.
- Develop and adopt "credible grade"-like metric for impressions", perhaps based on click signals

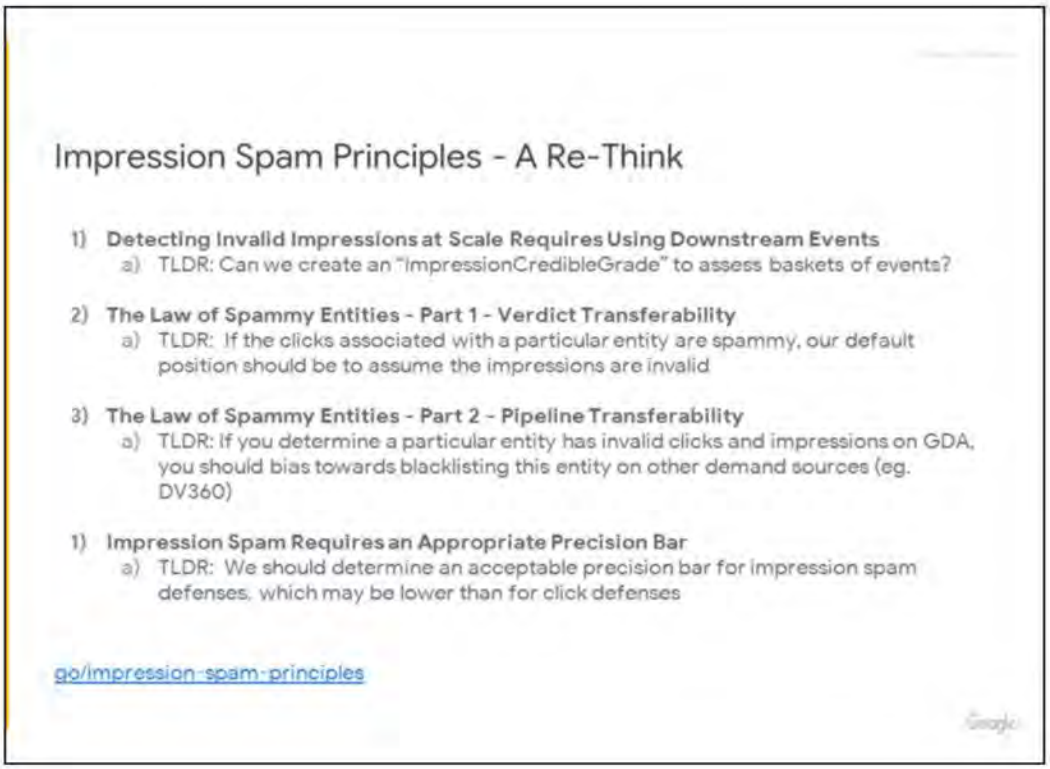
Google

Speaker: Arun

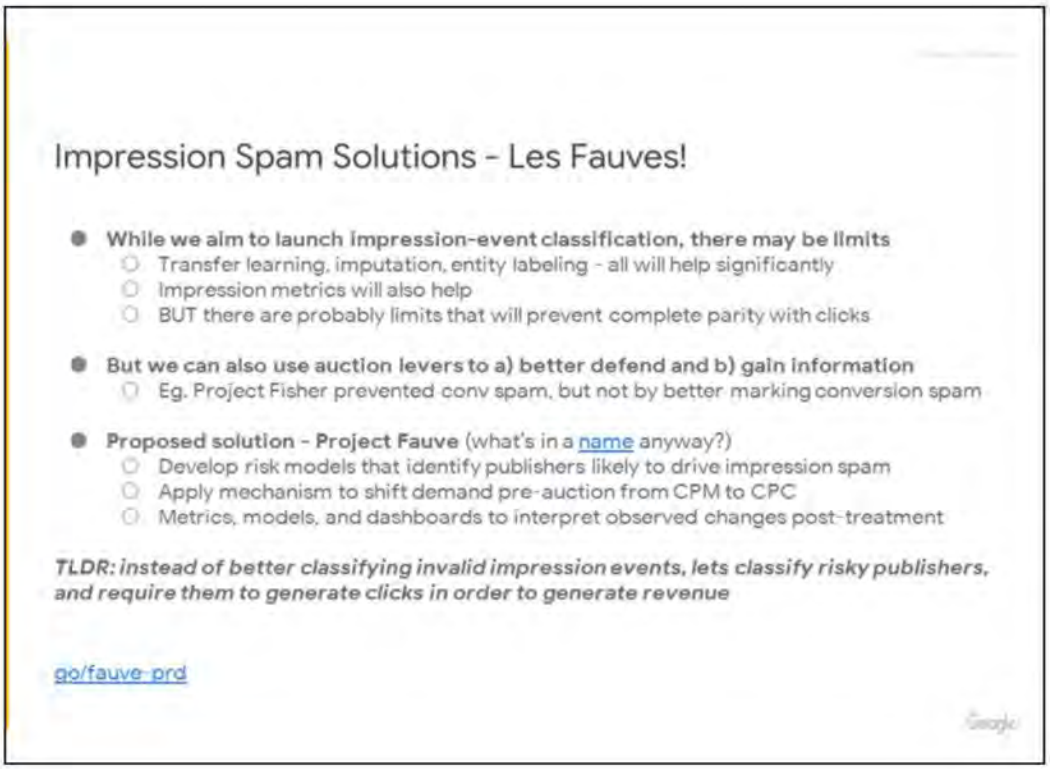
Speaker: Arun?



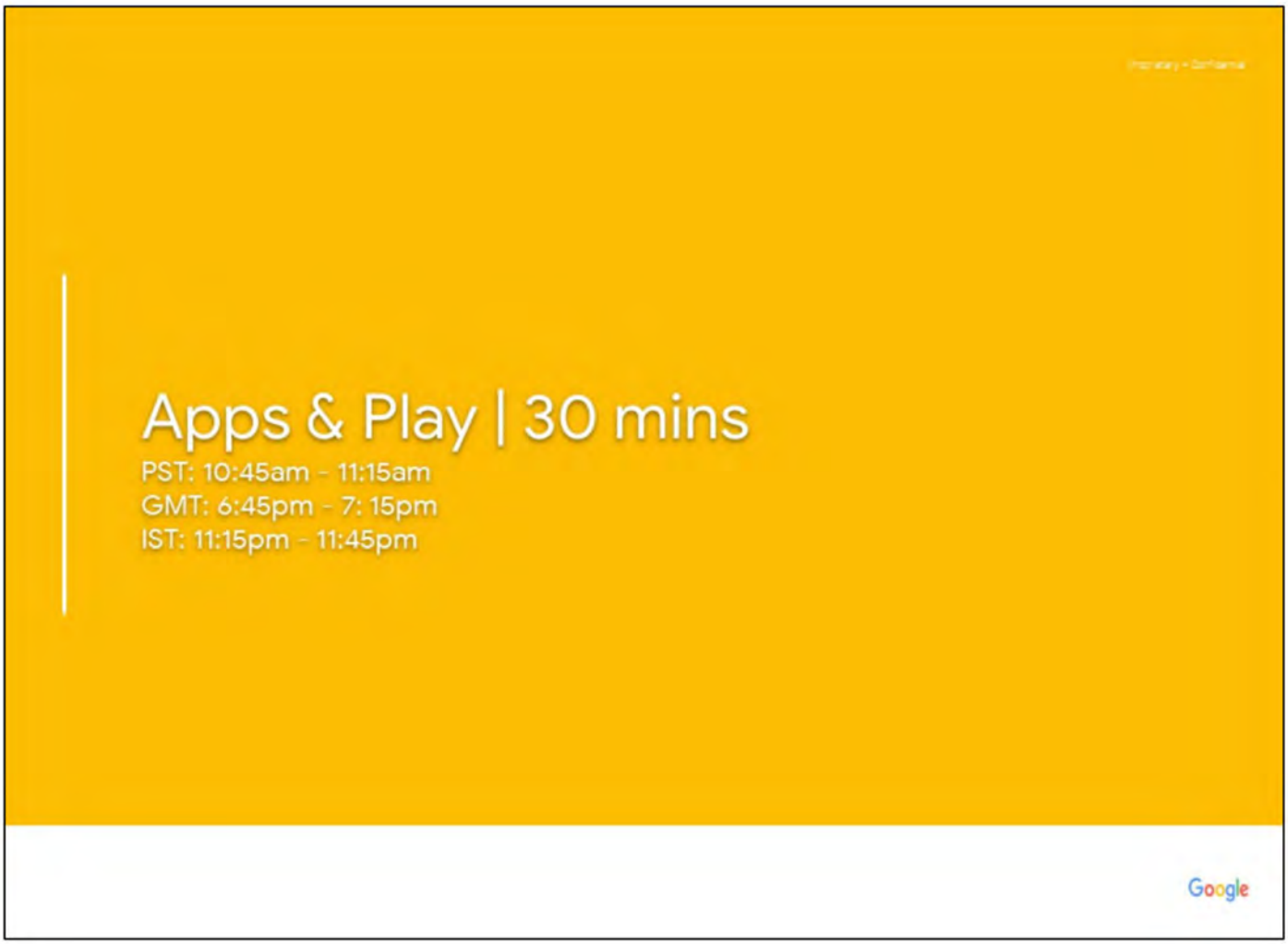
Speaker: Prachi

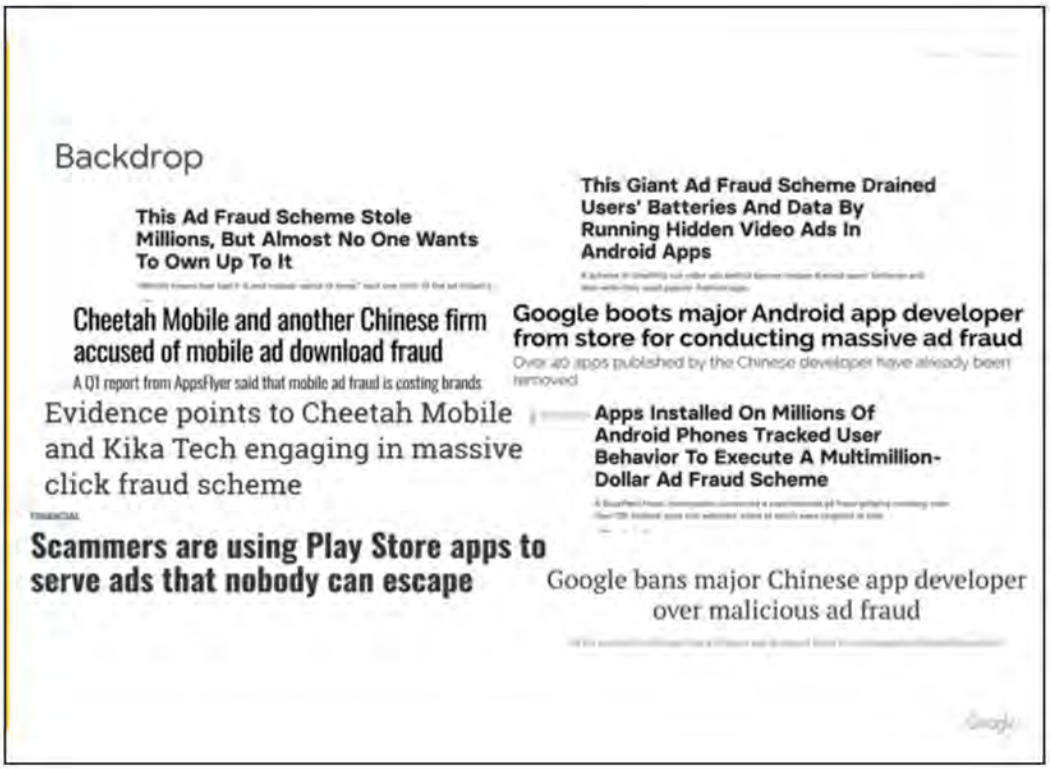


Speaker: Zack

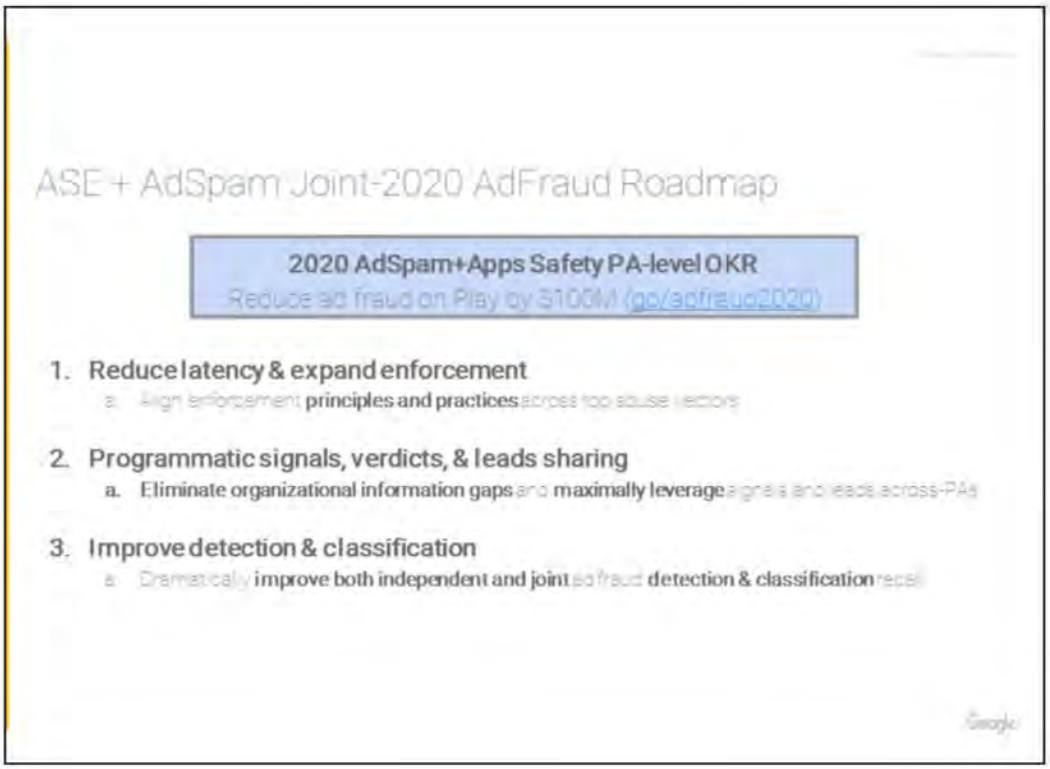


Speaker: Zack

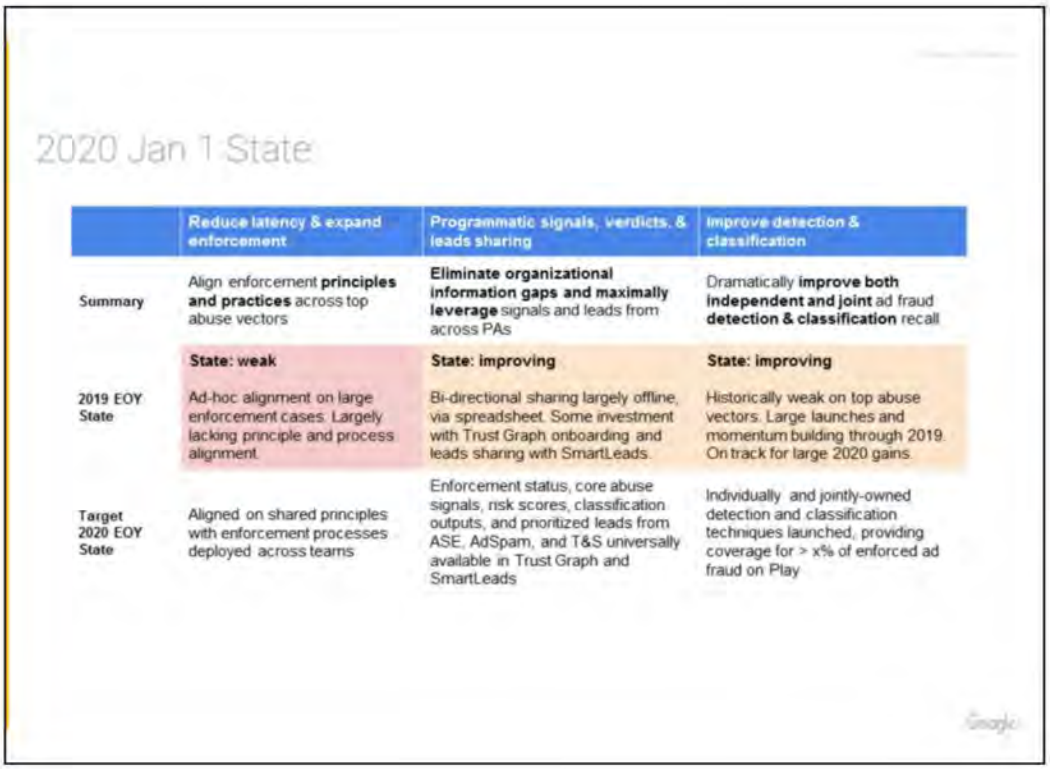

Apps & Play | 30 mins
PST: 10:45am - 11:15am
GMT: 6:45pm - 7: 15pm
IST: 11:15pm - 11:45pm
Google



Speaker: Zack



Speaker: Zack



2020 Jan 1 State

	Reduce latency & expand enforcement	Programmatic signals, verdicts, & leads sharing	Improve detection & classification
Summary	Align enforcement **principles and practices** across top abuse vectors	**Eliminate organizational information gaps and maximally leverage** signals and leads from across PAs	Dramatically **improve both independent and joint** ad fraud **detection & classification** recall
2019 EOY State	**State: weak** Ad-hoc alignment on large enforcement cases. Largely lacking principle and process alignment.	**State: improving** Bi-directional sharing largely offline, via spreadsheet. Some investment with Trust Graph onboarding and leads sharing with SmartLeads.	**State: improving** Historically weak on top abuse vectors. Large launches and momentum building through 2019. On track for large 2020 gains.
Target 2020 EOY State	Aligned on shared principles with enforcement processes deployed across teams	Enforcement status, core abuse signals, risk scores, classification outputs, and prioritized leads from ASE, AdSpam, and T&S universally available in Trust Graph and SmartLeads	Individually and jointly-owned detection and classification techniques launched, providing coverage for > x% of enforced ad fraud on Play

Speaker: Zack

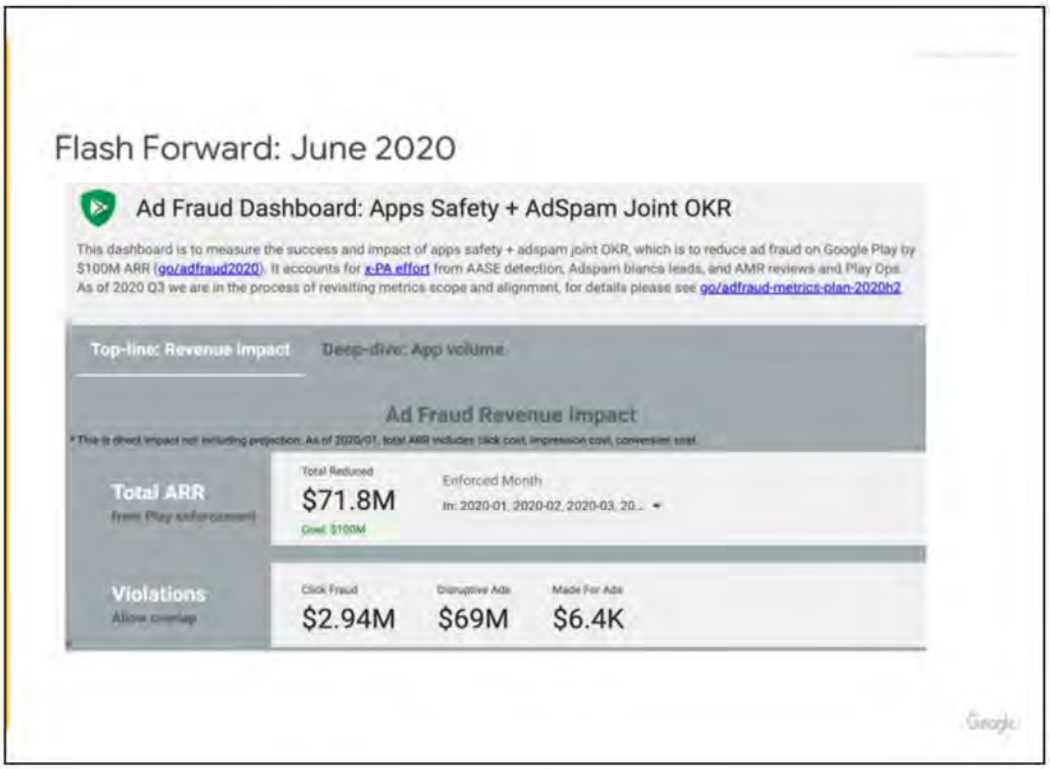
ASE + AdSpam Joint-2020 AdFraud Roadmap

	Reduce latency & expand enforcement	Programmatic signals, verdicts, & leads sharing	Improve detection & classification
Key Projects	• Launch joint-ad fraud enforcement principles • Shared T&S enforcement processes • Launch automated Marmot ortho scorer atop SmartLeads • Launch AdSpam pre-bid filter using ASE APK blacklists • On-device warnings for top abuse vectors	• Onboard top signal sharing use-cases onto Trust Graph • Onboard AdSpam, ASE and T&S app/dev classifications and enforcement verdicts onto Trust Graph • Launch SmartLeads to enable cross-PA leads and cluster sharing • Ad fraud focused 3P rewards program to help generate more leads/intelligence	• Launch new signal collection technologies to improve detection • Launch improved classifiers using new in-house and cross-PA signals and labels

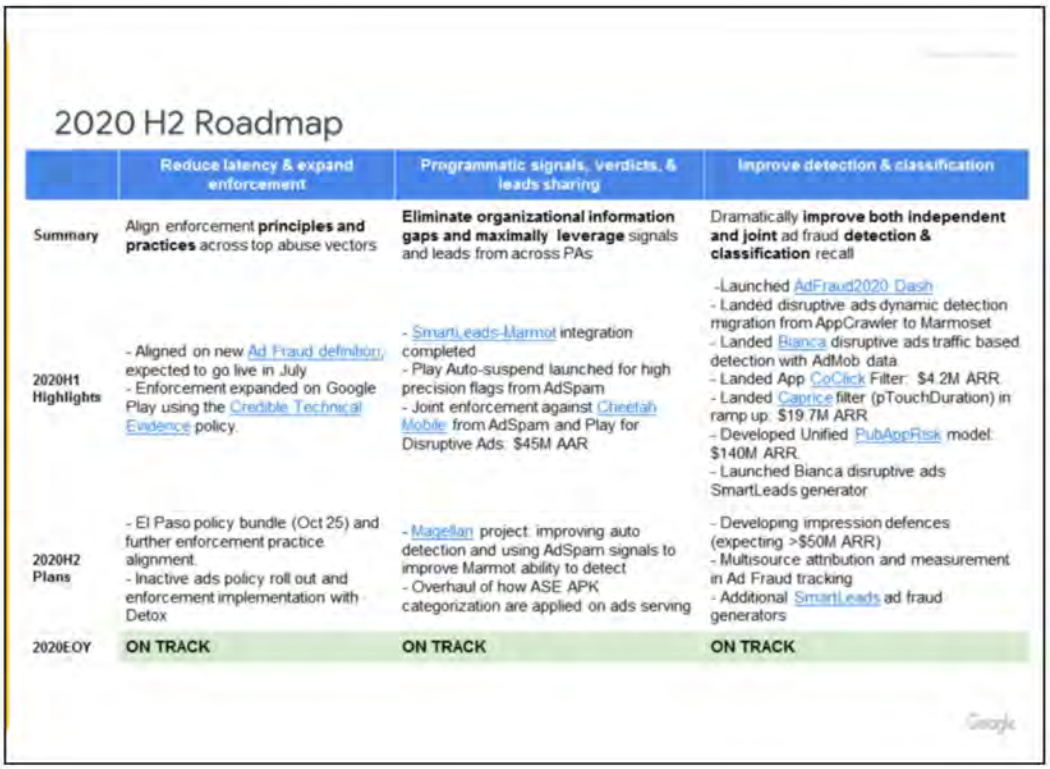
go/adfraud2020-roadmap

Google

Speaker: Zack



Speaker: Zack



2020 H2 Roadmap

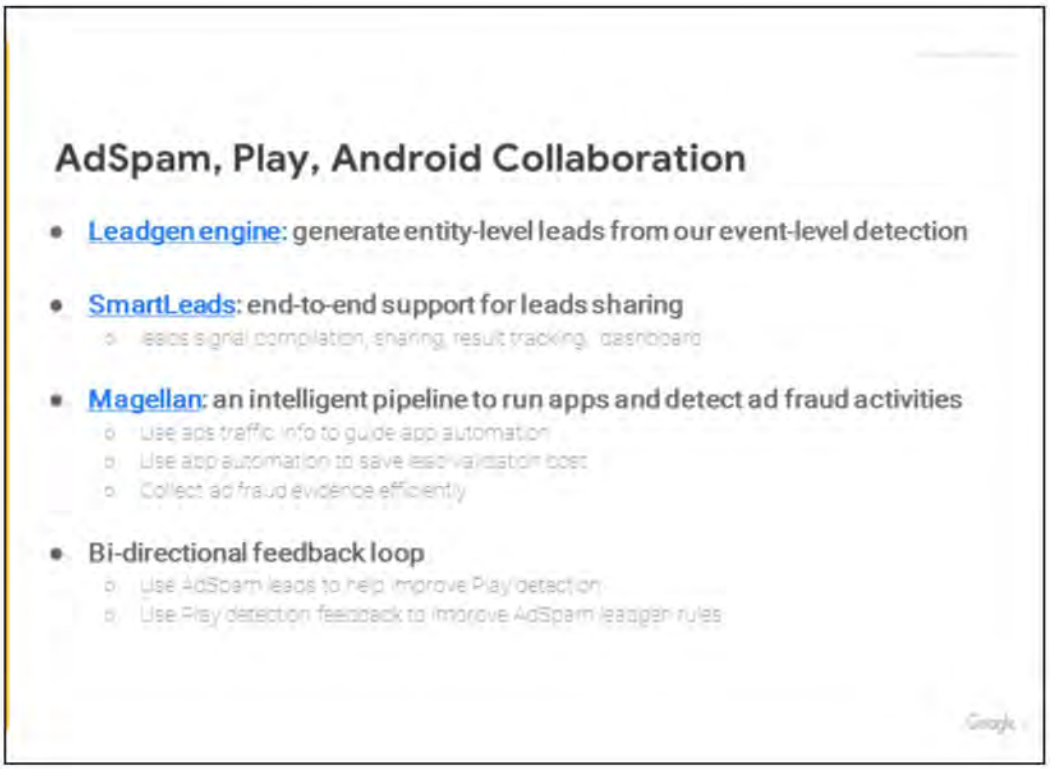
	Reduce latency & expand enforcement	Programmatic signals, verdicts, & leads sharing	Improve detection & classification
Summary	Align enforcement **principles and practices** across top abuse vectors	**Eliminate organizational information gaps and maximally leverage** signals and leads from across PAs	Dramatically **improve both independent and joint** ad fraud **detection & classification** recall
2020H1 Highlights	- Aligned on new Ad Fraud definition; expected to go live in July - Enforcement expanded on Google Play using the Credible Technical Evidence policy.	- SmartLeads-Marmot integration completed - Play Auto-suspend launched for high precision flags from AdSpam - Joint enforcement against Cheetah Mobile from AdSpam and Play for Disruptive Ads. $45M AAR	-Launched AdFraud2020 Dash - Landed disruptive ads dynamic detection migration from AppCrawler to Marmoset - Landed Bianca disruptive ads traffic based detection with AdMob data - Landed App CoClick Filter: $4.2M ARR - Landed Caprice filter (pTouchDuration) in ramp up. $19.7M ARR - Developed Unified PubAppRisk model: $140M ARR - Launched Bianca disruptive ads SmartLeads generator
2020H2 Plans	- El Paso policy bundle (Oct 25) and further enforcement practice alignment. - Inactive ads policy roll out and enforcement implementation with Detox	- Magellan project: improving auto detection and using AdSpam signals to improve Marmot ability to detect - Overhaul of how ASE APK categorization are applied on ads serving	- Developing impression defences (expecting >$50M ARR) - Multisource attribution and measurement in Ad Fraud tracking - Additional SmartLeads ad fraud generators
2020EOY	**ON TRACK**	**ON TRACK**	**ON TRACK**

Google

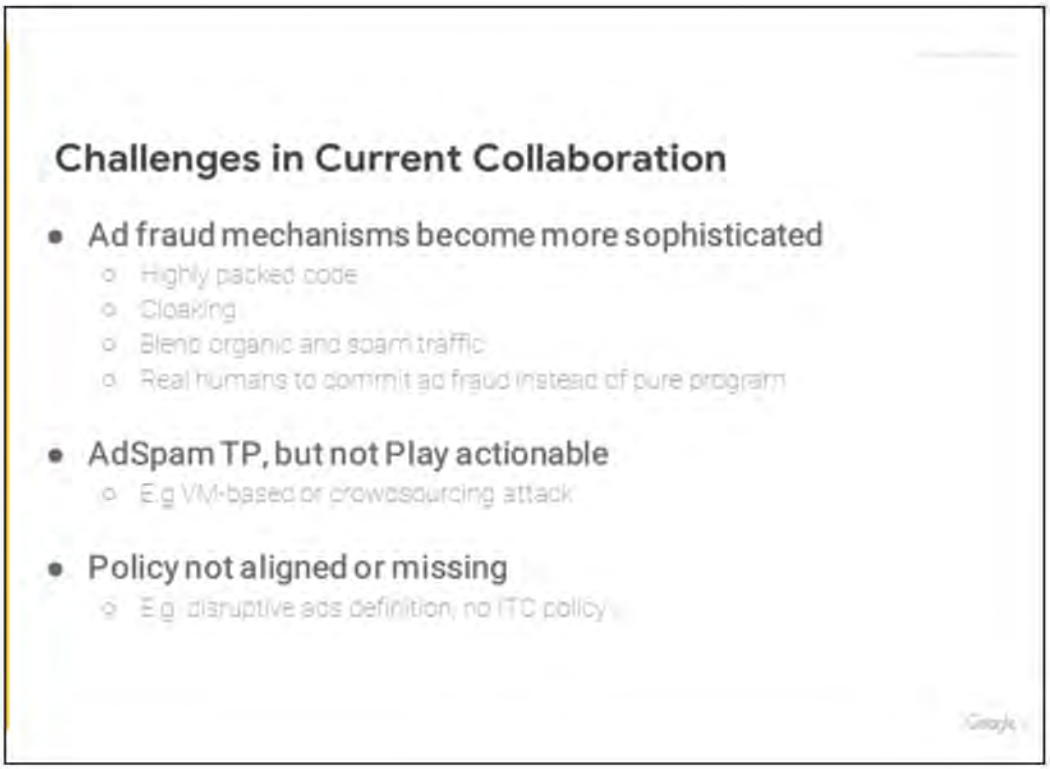
Speaker: Zack


Top Themes
Disruptive ads
Out of context ads
Current: out of context interstitials (outstitials)
Coming soon: out of context banners
No UI/Hidden icon apps
Coming soon: excessive ads
Click fraud
Current: direct AdShield signal detection
Coming: aggregated traffic analysis (e.g. pTouchDuration, pXY)
ITC (incentivized to click)
AdSpam has certain level of detection
Need Play policy to enforce at Play store
Impression Fraud

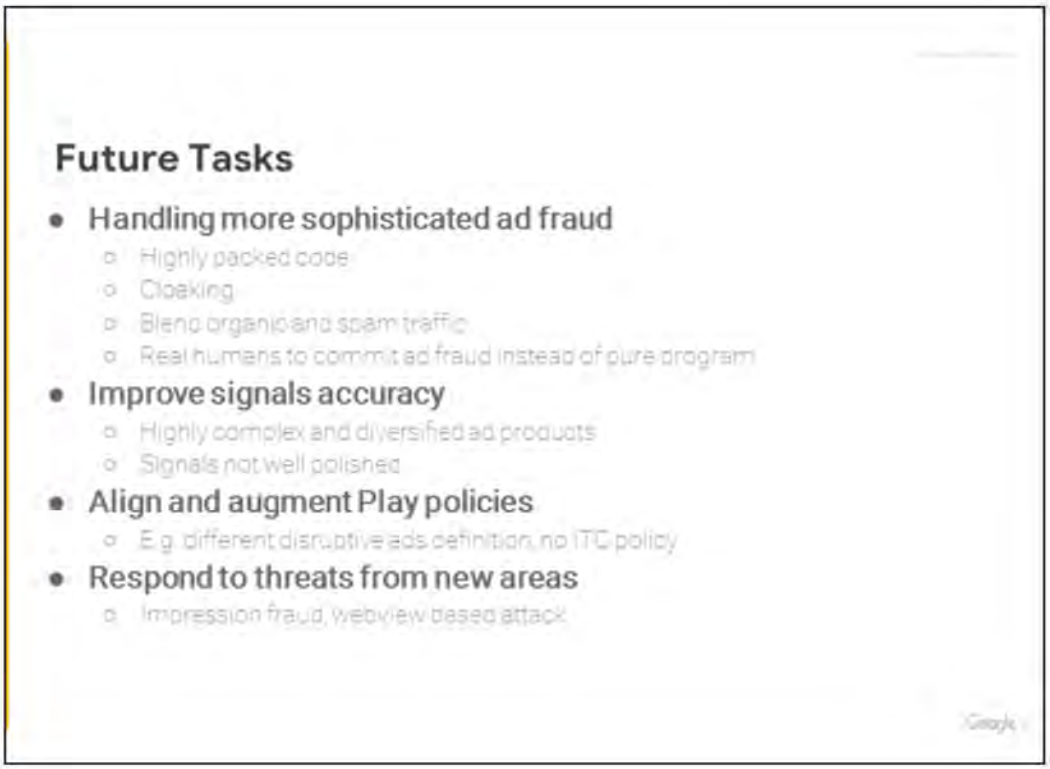
Speaker: Xin


AdSpam, Play, Android Collaboration
Leadgen engine: generate entity-level leads from our event-level detection
SmartLeads: end-to-end support for leads sharing
leads signal compilation, sharing, result tracking, dashboard
Magellan: an intelligent pipeline to run apps and detect ad fraud activities
Use ads traffic info to guide app automation
Use app automation to save lead validation cost
Collect ad fraud evidence efficiently
Bi-directional feedback loop
Use AdSpam leads to help improve Play detection
Use Play detection feedback to improve AdSpam leadgen rules

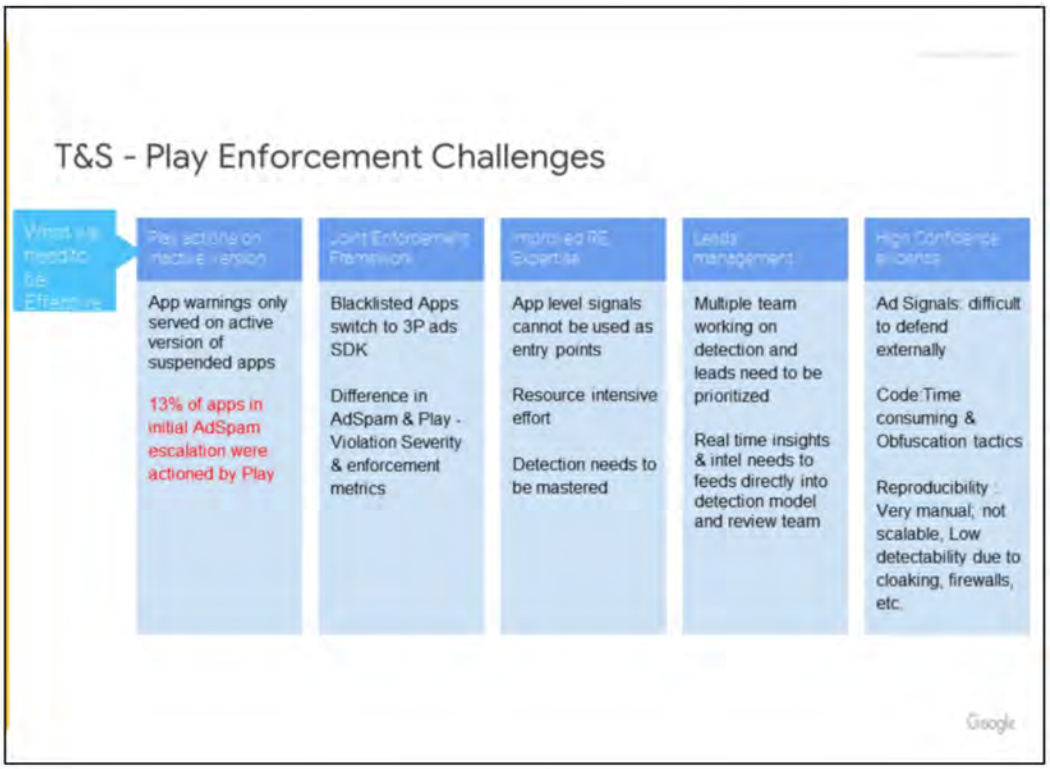
Speaker: Xin


Challenges in Current Collaboration
Ad fraud mechanisms become more sophisticated
Highly packed code
Cloaking
Blend organic and spam traffic
Real humans to commit ad fraud instead of pure program
AdSpam TP, but not Play actionable
E.g VM-based or crowdsourcing attack
Policy not aligned or missing
E.g. disruptive ads definition, no ITC policy

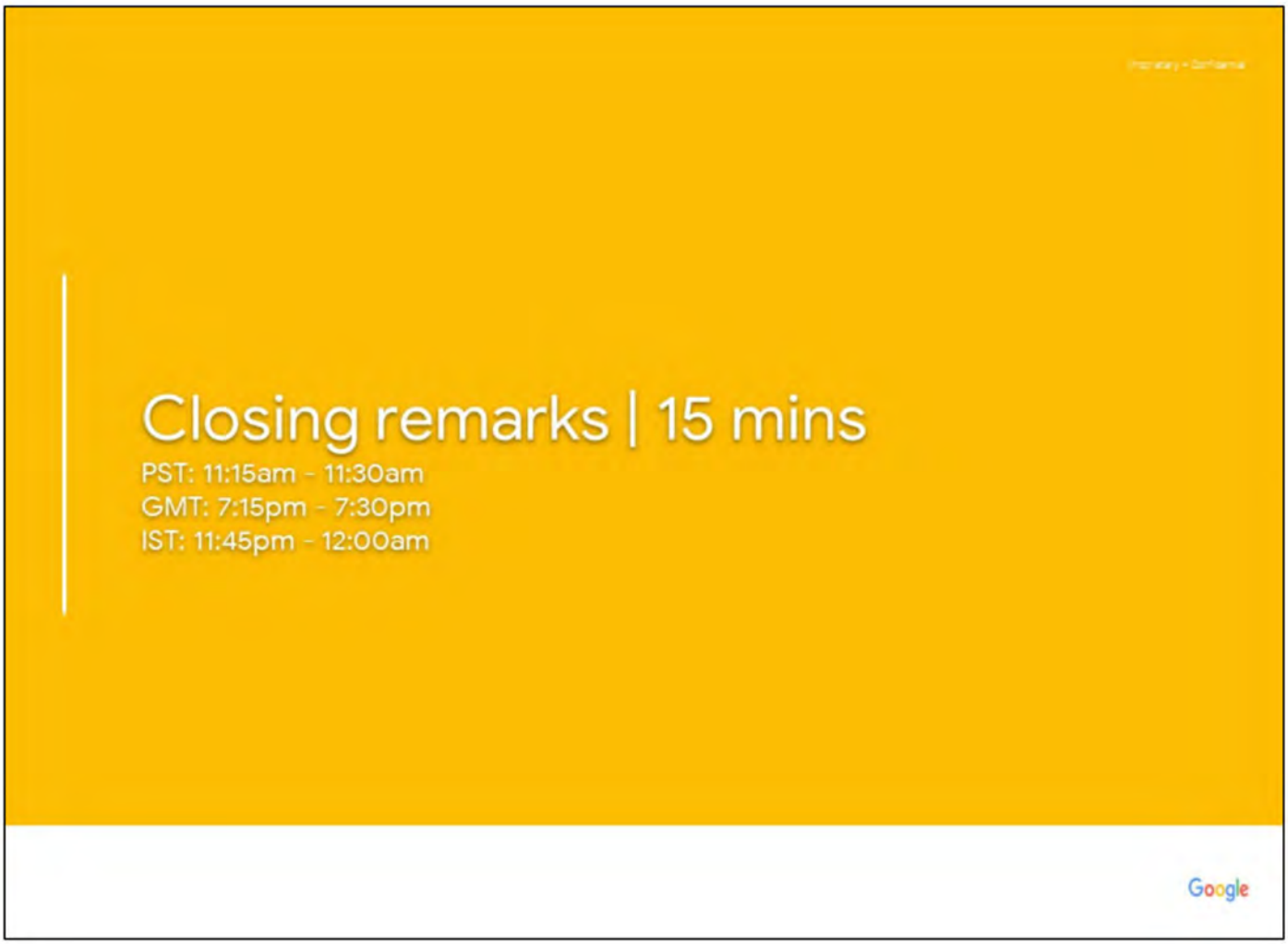
Speaker: Xin

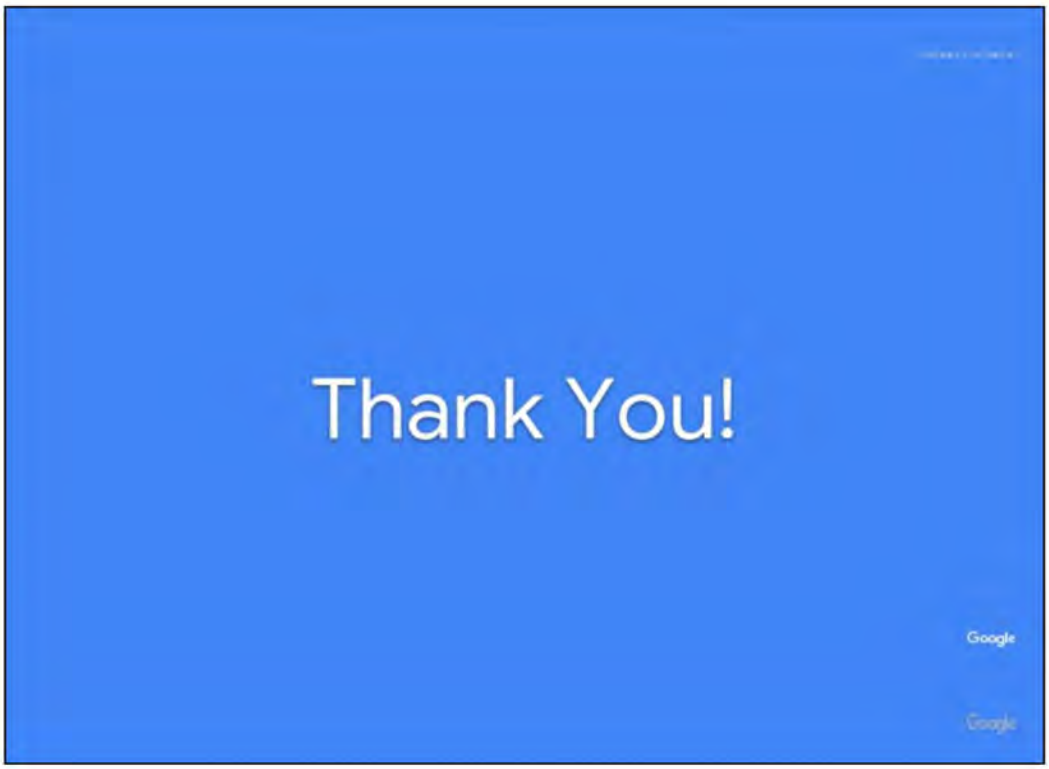

Future Tasks
Handling more sophisticated ad fraud
Highly packed code
Cloaking
Blend organic and scam traffic
Real humans to commit ad fraud instead of pure program
Improve signals accuracy
Highly complex and diversified ad products
Signals not well polished
Align and augment Play policies
E.g. different disruptive ads definition, no ITC policy
Respond to threats from new areas
Impression fraud, webview based attack

Speaker: Xin

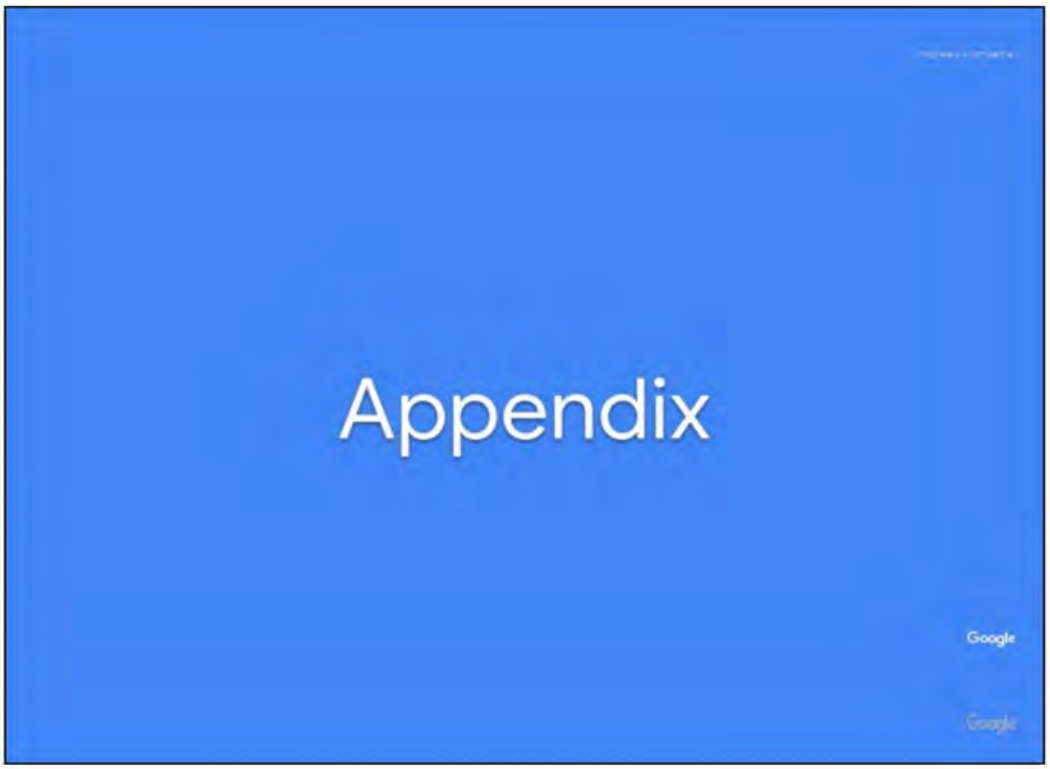


Speaker: Prachi


Closing remarks | 15 mins
PST: 11:15am - 11:30am
GMT: 7:15pm - 7:30pm
IST: 11:45pm - 12:00am
Google



Reminder to provide feedback



Reminder to provide feedback